PERSPECTIVES STRATÉGIQUES

POUR LA SANTÉ NUMÉRIQUE AU MAROC

GST · HAS · CNDP · MSPS

Cadre de gouvernance des données de santé :
référentiel stratégique pour la normalisation des pratiques nationales

NIA - POLICY BRIEFS - Volume 1 -

Association NIA
THINK TANK
Program D-NIA

Perspectives Stratégiques pour
la Santé Numérique au Maroc

CADRE DE GOUVERNANCE
DES
DONNÉES DE SANTÉ :

Référentiel Stratégique pour la Normalisation des Pratiques Nationales

National Institutional Acceleration
Association NIA – جمعية نية
التسريع المؤسساتي الوطني

Perspectives Stratégiques pour la Santé Numérique au Maroc (Volume 1 – Chapitre I).

Cadre de gouvernance des données de santé : référentiel stratégique pour la normalisation des pratiques nationales.

Référentiel stratégique de politiques publiques — *Policy Brief*

Association NIA (Éd.)

Résidence Al Mannar, Tabriquet
Immeuble n° 6-7, pépinière, 11000 Salé.
Site web : www.associationnia.org
Courriel : association.nia.maroc@gmail.com

Citation recommandée

Association NIA (Éd.). (2026). *Cadre de gouvernance des données de santé : référentiel stratégique pour la normalisation des pratiques nationales. Perspectives stratégiques pour la santé numérique au Maroc*, vol. 1. ISBN 978-9920-8729-1-1.

Informations bibliographiques

ISBN (e-book) : 978-9920-8729-1-1

Table des matières

— Informations éditoriale 5

— Préface 6

— Résumé exécutif 7

— Introduction 9

Recommandation I — Cadre de gouvernance des données de santé au sein des GST

1. Objectif 11

2. Principes fondamentaux 1

Recommandation II — Socle de données de santé clinique (Minimum Clinical Data Set)

1. Définitions et utilité stratégique 16

2. Étude du benchmark: le modèle français (Health Data Hub) 16

3. Proposition du MCDS marocain — Triple pilier de gouvernance 18

Recommandation III — Processus de gouvernance standard des données

1. Acquisition 22
2. Stockage 26
3. Usage 26
4. Diffusion et accès internes 27
5. Partage et diffusion externe 27
6. Archivage et suppression 28
7. Diagramme du cycle de vie des données 28

Recommandation IV — Renforcement des capacités légales

1. Objectif 30

2. Évaluation du cadre légale actuel 30

3. Renforcement du cadre légal 31

Recommandation V — Renforcement des capacités institutionnelles

1. Objectif 34

2. Évaluation des capacités institutionnelles 34

3. Mécanismes de renforcement 35

Recommandation VI — Échange et interopérabilité des données

1. Standards d'interopérabilité 38

2. Architecture des données 38

3. Gouvernance des flux- Principe *Zero Trust* 39

Recommandation VII — Gouvernance et opérationnalisation au niveau des GST

1. Structures locales 40

2. Procédures opérationnelles standardisées (SOP) 44

3. Délégué à la Protection des Données (DPO) 47

Recommandation VIII — Création et gouvernance des Entrepôts de Données de Santé (EDS) au niveau des GST

1. Contexte et levier des réformes sanitaires 51

2. Rôle et utilité stratégique des EDS 51

3. État des lieux au Maroc 52

4. Recommandations d'actions stratégiques 52

Feuille de route opérationnelle — Horizon 2026–2030

Contexte et principes directeurs 66

Matrice de gouvernance institutionnelle 67

Phase 1 — Validation du modèle de gouvernance numérique (Mois 1–18) 68

Phase 2 — Structuration de l'infrastructure nationale d'interopérabilité (Mois 19–36) 71

Phase 3 — Renforcement des capacités institutionnelles et humaines (Mois 25–42) 73

Phase 4 — Généralisation nationale à l'ensemble des GST (Mois 37–72) 75

Préparation organisationnelle transversale 77

Synthèse exécutive 77

Sections complémentaires

— Conclusion 79

— Bibliographie 81

— Table des annexes 85

— Glossaire des acronymes 88

INFORMATIONS ÉDITORIALES

ÉDITEUR

Association NIA – *Think tank* Politiques Publiques de Santé

DIRECTION SCIENTIFIQUE

Mme Youssra EL KHOULALI (dir.)

AUTEURS CONTRIBUTEURS

Mme Meryem JOUTE

Mme Nissrine EL YADOUNI

M. Yahya LAHRIMI

M. Nour ABOULFETH

Mme Hiba KOUDRI

Mme Rime TAZOUT

RELECTURE SCIENTIFIQUE

Pr. Sabrina GUETIBI

PRÉFACE

Depuis sa création en 2024, l'association NIA s'est donné une mission claire : catalyser la recherche scientifique appliquée au service du progrès national. Notre conviction fondatrice est simple — la science et la technologie sont les fondations de toute civilisation, et le Maroc a vocation à devenir un hub d'innovation compétitif à l'échelle mondiale.

C'est dans cet esprit que nous avons lancé notre programme : "Digital-National Institutional Acceleration" (D-NIA), dédié à l'incubation de projets de recherche et développement en santé numérique. Cette ambition doit beaucoup, à titre personnel, aux travaux de M. Daron Acemoglu et de ses coauteurs, distingués par le prestigieux prix Nobel d'économie 2024 pour leur démonstration lumineuse sur la formation des institutions et leur rôle dans la prospérité des nations. Leur thèse est limpide : la qualité des institutions, et leur caractère inclusif, conditionnent durablement la croissance économique et le développement d'un pays. Transposée à la santé, cette théorie du changement — centrée sur la gouvernance et la qualité institutionnelle du système — a nourri d'intenses réflexions au sein de notre équipe, dont beaucoup trouvent aujourd'hui une application concrète dans nos recommandations.

Face aux défis structurels de l'écosystème marocain de recherche et d'innovation en santé — au premier rang desquels la rareté des données mobilisables pour l'intérêt public —, nous avons créé le Think Tank Politiques Publiques de Santé. Cette initiative réunit des experts et chercheurs engagés dans un double exercice : porter une ambition pour l'avenir de la santé digitale au Maroc, et faire avancer, de manière pragmatique, notre théorie du changement face au statu quo.

Le Groupe de Travail qui en est issu formule des recommandations selon une approche *evidence-to-practice*, structurées autour de trois axes stratégiques — gouvernance des données de santé, déploiement de l'intelligence artificielle, et centre d'excellence en innovation — réunis dans notre série « Perspectives Stratégiques pour la Santé Numérique au Maroc ».

Nous invitons l'ensemble des acteurs concernés à s'approprier ces recommandations et à dialoguer avec nous. Nous restons à votre écoute.

YOUSSRA EL KHOULALI
PRÉSIDENTE, NIA

Résumé exécutif

La gouvernance des données de santé constitue le socle indispensable de la transformation numérique du système de santé, conditionnant la sécurité des informations, le respect des principes éthiques et le succès du déploiement de l'intelligence artificielle au sein des **Groupements Sanitaires Territoriaux (GST)**. Sans un cadre structuré, harmonisé et opérationnel, la donnée de santé ne peut jouer pleinement son rôle stratégique au service du pilotage public, de la recherche, de la qualité des soins et de l'innovation.

Ce référentiel stratégique vise à définir un cadre normatif et opérationnel garantissant la sécurité, la qualité, l'interopérabilité et la valorisation responsable des données de santé à l'échelle nationale, en alignement avec la réforme des GST et la stratégie « Maroc Digital 2030 », afin d'assurer une cohérence durable entre transformation numérique, politiques publiques de santé et souveraineté numérique.

Le diagnostic met en évidence des défis structurels majeurs : les systèmes d'information hospitaliers restent fragmentés et cloisonnés, limitant la circulation fluide des données et la continuité du parcours patient. L'absence d'un référentiel national unifié engendre des pratiques hétérogènes et des asymétries réglementaires entre établissements, accroissant la vulnérabilité des données et réduisant la capacité de pilotage, le développement de la recherche clinique et le déploiement de l'intelligence artificielle. Ces limites sont renforcées par un déficit de coordination institutionnelle et un manque d'outils de suivi et de redevabilité, compromettant la performance globale du dispositif numérique.

Pour répondre à ces enjeux, le référentiel propose quatre axes stratégiques complémentaires :

- **Modernisation du cadre légal et renforcement institutionnel** — notamment par l'adaptation de la loi 09-08 et le renforcement du rôle de la CNDP, y compris par l'octroi de pouvoirs de sanction directe.
- **Standardisation et structuration des données** — via un socle minimal de données cliniques et l'adoption de standards HL7 FHIR, pour unifier les systèmes d'information et garantir la traçabilité du parcours patient.
- **Sécurisation des flux et protection de la vie privée** — par une architecture Zero Trust, une gestion fine des accès et des mécanismes de traçabilité renforcés.
- **Renforcement des compétences** — soutenus par un programme national de formation continue et des indicateurs de performance harmonisés.

Le présent référentiel ambitionne de positionner les Groupements Sanitaires Territoriaux comme des catalyseurs d'un écosystème de santé apprenant, sécurisé, inclusif et centré sur le patient — constituant ainsi une condition déterminante de la crédibilité scientifique, de l'efficience du pilotage public et de la souveraineté numérique du Maroc dans le domaine de la santé, au service de l'intérêt général.

Introduction

Les données de santé représentent aujourd'hui un élément central pour tout système de santé moderne, au Maroc comme ailleurs, car elles nourrissent la qualité des soins, soutiennent l'innovation clinique et orientent les politiques publiques. Il s'agit de données à caractère personnel[1], relatives à la santé physique ou mentale d'une personne et incluent les prestations de soins, révèlent des informations sur son état de santé passé, présent ou futur[2]. En raison de leur nature sensible, elles constituent un objet de protection renforcée, indispensable pour garantir la confidentialité et la confiance des citoyens. Bien gouvernées, ces données dépassent le simple cadre administratif. En effet, elles permettent de piloter le système, d'anticiper les besoins des populations et de soutenir efficacement la recherche médicale. L'exercice d'une gouvernance rigoureuse et responsable devient ainsi un impératif national, concrétisé notamment à travers le déploiement des GST, qui instaurent une coordination régionale et un cadre institutionnel robuste pour sécuriser, harmonier et valoriser l'information médicale.

Cependant, cette restructuration territoriale ne saurait se limiter à une simple modernisation administrative. Elle soulève un enjeu de souveraineté numérique majeur. Dans un contexte mondial où la donnée est devenue une ressource stratégique convoitée, la capacité du Maroc à maîtriser, protéger et exploiter son patrimoine informationnel de santé détermine son indépendance technologique. L'absence actuelle d'une architecture de données unifiée ne crée pas seulement des inefficacités opérationnelles mais expose le système national à une dépendance vis-à-vis de solutions exogènes. Cette situation est d'autant plus critique que le recours à des prestataires technologiques dont les activités sont délocalisées peut soustraire les données au contrôle de la législation nationale[3], rendant la protection des citoyens incertaine. En l'absence d'une gouvernance souveraine, l'implication inévitable des géants mondiaux du numérique dans les infrastructures de santé risque de compromettre définitivement l'indépendance technologique du pays[4].

D'un autre côté, le paysage actuel des systèmes d'information hospitaliers se caractérise par une dispersion quasi endémique où les outils, souvent propriétaires et limités à un accès local, engendrent une hétérogénéité dans les écosystèmes existants[5]. Ce cloisonnement profond est le symptôme manifeste de l'absence d'un système unifié d'information partagé[6], une situation où, faute de référentiel commun, chaque entité finit par parler sa propre langue. Ainsi, cette désarticulation structurelle produit une information médicale souvent redondante, désorganisée, décousue et inaccessible[7], ce qui fragilise gravement la fiabilité des données et les expose à des risques accrus d'inexactitude. En définitive, l'information reste confinée dans des silos organisationnels rigides et jalousement gardée comme une ressource de pouvoir plutôt que cultivée comme un actif public partagé. Un tel contexte entrave substantiellement toute tentative de mutualisation, au détriment de la recherche, de l'innovation et d'un pilotage stratégique cohérent du système de santé à l'échelle nationale.

Face au contexte actuel, les données de santé sont un patrimoine auxquelles une attention particulière devrait être prêtée, surtout avec la prédominance de l'intelligence artificielle, et le recours intensifié au *Big Data*. Dès lors, la structuration de ce patrimoine est stratégique[8] afin d'en tirer pleinement les avantages qui en découlent et d'éviter les risques qui en résultent. En effet, l'intégration prospective et graduelle des technologies des traitements automatisés dans le système de santé constitue sans moindre doute un tournant

majeur et non redoutable pour le système de santé marocain, en ce qu'elle permet de promouvoir l'expérience du patient dans les établissements sanitaires notamment en améliorant la qualité du diagnostic, en optimisant la prise de décision médicale et en favorisant une personnalisation accrue des soins. Or, ces avancées ne pourraient aboutir sans un apprentissage fiable, sécurisé, et robuste des systèmes d'intelligence artificielle.

Dès lors, assez prometteuse qu'elle semble, cette situation est révélatrice de risques préoccupants, spécialement s'agissant de l'atteinte à la vie privée des personnes. Laquelle se trouve mise en péril durant toutes les étapes du cycle de la donnée, passant de la collecte, le traitement et l'analyse[9]. Par ailleurs, et malgré les avancées en matière de sécurité, notamment par la sophistication et la robustesse des systèmes de stockage et de traitement, leur vulnérabilité demeure une réalité[10] qui hante des données sensibles, telles celles relatives à la santé des personnes.

Face au dilemme des avantages prometteurs et des risques préoccupants, s'inscrit l'objet de ce chapitre, ayant vocation à tracer les contours d'une stratégie nationale de gouvernance des données de santé, en recommandant ses composantes clés, tout en s'accommodant avec les exigences et standards internationaux. Les recommandations ont ainsi mis en lumière une feuille de route pour une gouvernance des données dans le domaine sanitaire, en insistant de prime abord sur la nécessité de la détermination d'un cadre de gouvernance cerné par des principes fondamentaux tels, l'engagement des différents acteurs et parties prenantes bien ceux existants que ceux futurs, la coordination entre ces derniers, l'engagement dans le suivi continu de la mise en place effective des plans d'actions dans ce sens, etc...En outre, modèle organisationnel clair, permettant une gestion efficace et sécurisée des données, allant de l'acquisition, l'interopérabilité, le stockage à l'échange tenant compte des normes et standards internationaux. De surplus, les recommandations ont mis en lumière la nécessité d'assurer un accompagnement juridique renforcé, basé sur l'actualisation et la consolidation du cadre légal de référence, lié aux données, en l'occurrence la loi 09-08 relative à la protection des personnes physiques à l'égard, ainsi qu'au renforcement des capacités institutionnelles des organismes chargés de sa mise en œuvre, et de contrôle à sa conformité.

I. Première recommandation : Cadre de gouvernance des données de santé au sein des GST

1. Objectif

Le présent cadre vise à établir une gouvernance nationale cohérente, transparente et sécurisée des données de santé au sein des GST. Il a pour objectif d'assurer la gestion responsable, éthique et efficiente des informations de santé, en favorisant leur utilisation optimale au service de la planification, de la recherche et de l'amélioration continue de la qualité des soins.

Ce cadre a également pour vocation de renforcer la coordination entre les différents acteurs du système de santé, d'harmoniser les pratiques de gestion des données et de garantir la conformité aux exigences légales et réglementaires en matière de protection des données personnelles. En plaçant la confiance, la sécurité et la transparence au cœur de la gouvernance, il soutient la construction d'un écosystème numérique intégré, garantissant la souveraineté sanitaire nationale et contribuant au développement d'une santé publique plus équitable, innovante et résiliente.

2. Principes fondamentaux

Principe 1 — Participation inclusive et engagement des parties prenantes

Une gouvernance solide et équitable des données de santé constitue l'un des fondements d'un système de santé résilient et capable de s'adapter aux besoins de la population. Elle doit reposer sur une participation active et inclusive de l'ensemble des acteurs concernés, au premier rang desquels figurent les patients, détenteurs légitimes de leurs données de santé. Cette gouvernance associe les professionnels de santé, qui interviennent dans la collecte et l'utilisation des données dans le cadre de leurs missions de soins, sous l'égide et la responsabilité des GST. En tant qu'entités organisatrices du système de soins à l'échelle territoriale, les GST constituent les acteurs centraux et responsables du traitement des données de santé, assurant la coordination des établissements, la gestion des systèmes d'information et des entrepôts de données, ainsi que la mise en œuvre opérationnelle des politiques nationales de gouvernance.

Cette gouvernance implique également les autorités publiques et les instances de régulation, en particulier la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel (CNDP), qui veille à la conformité légale des traitements, à la protection des droits des personnes et à l'effectivité des garanties prévues par la loi. L'implication coordonnée de ces parties prenantes majeures, aux côtés des chercheurs et de la société civile, favorise des processus décisionnels transparents et inclusifs, fondés sur une répartition claire des rôles, des responsabilités et des mécanismes de contrôle. Elle renforce la redevabilité institutionnelle et la confiance publique, en garantissant que les données de santé, en raison de leur sensibilité particulière, soient collectées, traitées et valorisées de manière sécurisée, éthique et proportionnée, exclusivement au service du bien commun, de la qualité des soins et de l'intérêt général.

Principe 2 — Coordination et coopération institutionnelle

Une coordination entre tous les acteurs du système est la clé de voûte d'une gouvernance efficace. C'est ainsi que les autorités publiques, les Groupements Sanitaires Territoriaux, les institutions de recherche et les organismes de régulation doivent coopérer de manière harmonisée afin d'assurer l'alignement des politiques, une interopérabilité fluide des systèmes et une continuité ininterrompue du service public de santé. Cette coopération institutionnelle doit être soutenue par des mécanismes de partage d'informations sécurisés, conformes aux normes légales de protection des données personnelles, afin de garantir la circulation fluide des informations entre acteurs et d'éliminer les silos institutionnels. De tels mécanismes de coordination et de coopération renforcent la solidité du cadre national de gouvernance des données de santé, garantissent une application uniforme des normes, procédures et bonnes pratiques ainsi qu'ils optimisent la gestion des ressources et la mutualisation des compétences.

Principe 3 — Développement de la maturité digitale et organisationnelle

La gouvernance efficace des données de santé repose sur la capacité des parties prenantes, notamment les GST, à évaluer et à renforcer leur maturité numérique, juridique et organisationnelle. En effet, chaque acteur du système doit identifier ses écarts par rapport aux exigences d'une gestion responsable des données, clarifier ses rôles et responsabilités, et mettre en place des mécanismes adaptés pour sécuriser, structurer et piloter l'ensemble des flux de données. Cette démarche constitue une condition préalable pour garantir la qualité, la fiabilité et la protection des données tout au long de leur cycle de vie, tout en assurant leur conformité aux principes éthiques et réglementaires.

Pour atteindre ces objectifs, il est essentiel de développer et d'adopter des infrastructures, des outils et des compétences adaptés, couvrant des domaines tels que la cybersécurité, l'interopérabilité des systèmes, la gestion des consentements et la formation continue des professionnels. La mutualisation des expertises et la modernisation coordonnée des infrastructures permettent de dépasser une approche fragmentée et purement technologique, pour instaurer une gouvernance intégrée et proactive des données de santé. Ce principe vise à transformer les données en un actif stratégique fiable, favorisant l'innovation, l'efficacité opérationnelle et la prise de décision éclairée dans l'ensemble du système de santé.

Principe 4 — Transparence et information du public

La transparence constitue un fondement essentiel, tant au niveau national qu'international, d'une gouvernance responsable des données de santé, exigeant que le public, notamment les patients, soit informé de manière claire et exhaustive sur les finalités multiples, les risques potentiels et les bénéfices tangibles liés à la collecte et à l'utilisation de leurs données sensibles. Cette approche favorise une compréhension profonde et un accès équitable à des informations intelligibles et disponibles dans plusieurs langues pour éliminer les barrières culturelles et promouvoir une inclusion totale. Au-delà de la dimension individuelle, la transparence s'étend à une dimension sociétale. En assurant que la gestion se fait dans le respect de la transparence, la confiance collective dans les politiques institutionnelles se renforce naturellement.

Principe 5 — Consentement et bases légales de traitement

Le traitement des données de santé doit reposer sur des fondements juridiques clairs, transparents et conformes aux normes nationales et internationales. Le consentement éclairé des individus demeure une base essentielle, garantissant le respect de leur autonomie et de leur droit à la vie privée. Toutefois, la gouvernance des données de santé reconnaît également d'autres bases légales de traitement, notamment la mission d'intérêt public, l'obligation légale ou la nécessité de protéger la santé publique. Le recours à ces bases doit toujours s'accompagner de garanties strictes assurant la légitimité, la proportionnalité et la sécurité du traitement des données.

Le consentement éclairé implique que chaque individu soit informé de manière claire, complète et compréhensible des finalités du traitement, des acteurs impliqués, des modalités de conservation et des droits dont il dispose, notamment celui de retrait. Dans les situations où le consentement individuel n'est pas praticable, des mécanismes alternatifs de transparence et de supervision doivent être mis en place afin de préserver la confiance du public. Cette approche équilibrée permet de concilier la protection des droits individuels avec les impératifs collectifs de santé publique et de recherche, consolidant ainsi la légitimité du cadre national de gouvernance des données de santé.

Principe 6 — Revue éthique, approbation scientifique et suivi continu

Toute utilisation secondaire des données de santé, qu'elle concerne la recherche scientifique, la planification sanitaire stratégique ou le développement de technologies avancées, doit être soumise à un processus rigoureux d'évaluation scientifique, juridique et éthique, visant à garantir la conformité aux lois et règlements en vigueur, à prévenir les risques de réidentification et à s'assurer que l'utilisation des données soit justifiée, proportionnée et bénéfique. Cette revue préalable devrait s'accompagner de mécanismes d'approbation transparents et documentés, impliquant une évaluation minutieuse des impacts potentiels, une traçabilité complète des décisions et une protection des droits individuels au sein des Groupements Sanitaires Territoriaux. En intégrant ces mécanismes dans chaque phase du cycle de vie des données, les institutions s'assurent que toute utilisation respecte les principes de légalité, de pertinence et de sécurité.

Parallèlement, un dispositif de suivi postérieur au traitement des données devrait être mis en place et reposerait sur la mise en place d'audits réguliers qu'ils soient internes, effectués notamment par les GST, ou externes, réalisés par les autorités de régulation. Le but est d'évaluer l'efficacité des pratiques et des performances en signalant notamment tout incident ou non-conformité aux lois en vigueur afin d'identifier les faiblesses, corriger les écarts et assurer l'application effective des normes de sécurité et de qualité. Par ailleurs, d'autres mécanismes de régulation et d'alerte, impliquant directement les propriétaires des données, sont mis en place pour signaler les anomalies et proposer des améliorations, instaurant ainsi une boucle d'apprentissage continue. Ainsi, la publication transparente des résultats d'audit renforce la redevabilité et soutient une culture de supervision proactive, assurant que l'ensemble du cycle de vie des données demeure constamment contrôlé et aligné sur les principes de légalité, de sécurité et de performance.

Principe 7 — Sécurité et protection des données

La protection des données à caractère personnel est une exigence absolue reposant sur l'implémentation des mesures techniques et organisationnelles solides. Cela inclut notamment le chiffrement pour protéger les informations, la pseudonymisation et l'anonymisation pour masquer les identités, le contrôle des accès pour limiter qui peut accéder aux données, ainsi que la journalisation régulière pour suivre les activités et la notification rapide des incidents. L'intégrité de ce dispositif impose que les infrastructures fassent l'objet d'audits réguliers pour prévenir efficacement les risques cybernétiques. En cas de violation avérée, la transparence impose une notification tant aux autorités, qu'aux personnes concernées. Ceci renforce la confiance des patients et garantit une gouvernance sécurisée des données au service de la santé publique.

Principe 8 — Formation et développement des compétences

Le personnel de santé, les chercheurs et toute personne impliquée dans le traitement des données doivent suivre des programmes de formation continue portant sur la gouvernance, l'éthique et la sécurité des données. Dès lors, investir dans le capital humain par les institutions, notamment les universités et les GST, est primordial afin d'assurer une maîtrise constante des données et de leurs traitements. La collaboration entre acteurs académiques, professionnels et institutionnels favorise le développement d'un langage commun et la diffusion d'une culture partagée de la donnée, fondée sur la responsabilité, la transparence et la rigueur scientifique. Cette culture doit encourager l'apprentissage interdisciplinaire, la mise à jour régulière des compétences techniques et la compréhension des enjeux juridiques liés à l'utilisation des données de santé. Le développement de cette expertise collective constitue ainsi un levier essentiel pour soutenir une gouvernance des données durable et souveraine.

Principe 9 — Nécessité et proportionnalité des données

Le traitement des données de santé doit se limiter strictement à ce qui est nécessaire pour atteindre les objectifs légitimes et clairement définis de la gouvernance sanitaire. Les informations collectées et utilisées doivent être adéquates, pertinentes et non excessives au regard des finalités poursuivies. Ce principe impose une évaluation préalable de la nécessité de chaque donnée collectée et une justification explicite de son utilisation. La proportionnalité du traitement doit être assurée à toutes les étapes, afin d'éviter toute collecte ou conservation superflue et de garantir un usage mesuré, respectueux des droits fondamentaux des individus.

La mise en œuvre de ce principe repose sur des mesures organisationnelles et techniques telles que la pseudonymisation, l'anonymisation, la limitation de l'accès aux données sensibles et la suppression automatique après la période de conservation requise. En intégrant ces exigences dans la conception même des systèmes et processus, les institutions assurent une protection efficace tout en maintenant la pertinence et la qualité des données utilisées. Ce principe constitue ainsi un pilier de confiance et de légitimité pour la gouvernance des données de santé.

II. Deuxième recommandation : Socle de données de santé clinique (*Minimum Clinical Data Set*)

1. Définitions et utilité stratégique

Définition : Le socle de données de santé clinique (MCDS) constitue un ensemble cohérent et standardisé d'éléments de données cliniques explicitement définis, collectés de manière systématique pour assurer l'interopérabilité, la traçabilité et la valorisation des données de santé.

L'importance stratégique de ce socle de données repose sur plusieurs piliers fondamentaux ; il constitue un instrument de standardisation des pratiques cliniques en garantissant que les mêmes variables sont collectées de manière uniforme à travers différents établissements hospitaliers[11]. Cette harmonisation facilite la comparabilité des données entre structures de soins, permettant ainsi des analyses épidémiologiques robustes et l'identification de variations dans les pratiques cliniques. Sur le plan de la recherche clinique, le socle de données de santé clinique représente un levier essentiel pour la constitution de cohortes et l'exploitation secondaire des données en vue d'améliorer la qualité des soins[12], d'autant plus qu'il facilite l'intégration de données issues de sources multiples et soutient le développement d'outils d'intelligence artificielle en santé en fournissant des data sets structurés et de haute qualité[13]. Cette approche soutient également les objectifs de médecine de précision en permettant l'exploitation de données pour personnaliser les parcours de soins. L'initiative OSIRIS à titre d'exemple en oncologie illustre cet avantage : son socle de données cliniques et génomiques a été conçu pour accélérer le partage de données essentielles à la prise en charge personnalisée des patients. En disposant de données cliniques standardisées à grande échelle, il devient possible de croiser efficacement ces informations et d'identifier des biomarqueurs ou profils de patients (par exemple via des algorithmes de *data mining*), améliorant ainsi la personnalisation des traitements[14].

2. Étude du benchmark : le modèle français (Health Data Hub)

La France constitue une référence internationale en matière de gouvernance des données de santé grâce à la création du *Health Data Hub* (HDH) en 2019. Cette plateforme a pour but de réunir, organiser et mettre à disposition les données du système national des données de santé mentionné à l'article L.1461-1 du code de la santé publique, modifié par la loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé en France et de promouvoir l'innovation dans l'utilisation des données de santé[15]. Cette plateforme nationale a pu couvrir 98,8 % de la population française, soit plus de 66 millions de personnes[16], et a pu développer un socle commun de données cliniques qui constitue une référence généraliste pour soutenir la gestion des établissements de santé, l'évaluation des parcours et des pratiques de soins, et comprend des données démographiques, cliniques, biologiques et thérapeutiques collectées de manière structurée et fiable au sein des systèmes d'information hospitaliers.

Le socle commun de ce modèle comprend 5 familles principales de variables qui peuvent être groupées ou

séparées en items spécifiques :

1. Données démographiques : identité du patient, lieu de résidence, couverture sociale.
2. Données du Programme de Médicalisation des Systèmes d'Information (PMSI) : informations médico-économiques d'hospitalisation, qui représentent les informations médico-administratives standardisées, collectées pour chaque hospitalisation afin de décrire l'activité des hôpitaux et de permettre des analyses médico-économiques[17].
3. Données biologiques : résultats d'examens de laboratoire standardisés.
4. Données du médicament : traitement pharmaceutique et éléments de posologie.
5. Données d'examens cliniques : observations médicales structurées et constantes vitales[18].

Les recommandations de la Health Data Hub sont notamment (Doctrine technique du numérique en santé [19]) :

- L'établissement des standards appropriés pour agréger les données, avec une documentation précise des items permettant leur bonne identification par les établissements.

- La clarification du cadre réglementaire de rapprochement entre bases de données, en particulier concernant les procédures d'anonymisation et les règles d'accès.

- Utilisation de référentiels terminologiques standardisés incluant :

Référentiel	Usage
ICD-10 (CIM-10)	Classification des diagnostics
SNOMED CT	Concepts cliniques
LOINC	Identification des tests de laboratoire
ATC	Classification des médicaments

Concernant le suivi des données et l'assurance qualité, le HDH et les entrepôts de données hospitaliers français se sont dotés de mécanismes rigoureux de suivi de la qualité et de la complétude des données du socle. Ces entrepôts sont définis par le Référentiel de maturité des entrepôts de données de santé (HDH, 2022) comme étant des plateformes internes aux établissements de santé permettant l'intégration, la structuration et la mise à disposition des données de santé issues des systèmes d'information hospitaliers, dans une logique de réutilisation secondaire[20].

3. Proposition du MCDS marocain — Triple pilier de gouvernance

Un modèle de socle minimal de données cliniques (MCDS) qui se base sur trois piliers essentiels et primordiaux est nécessaire. Nous recommandons d'allier un triple pilier de gouvernance dans ce modèle marocain de MCDS :

Pilier 1 : Base juridique claire

Le Maroc dispose d'un terrain juridique assez fort en ce qui concerne la protection des données à caractère personnel. En effet, la loi n° 09-08[21] établit les principes de base pour la protection des données personnelles au Maroc, imposant des obligations strictes de collecte, traitement et stockage des données. Cette loi désigne la CNDP comme l'autorité responsable de veiller à la conformité légale. D'un autre côté, la loi 05-20[22] relative à la cybersécurité et d'autres lois couvrent les infractions liées aux systèmes de traitement automatisé de données, les transactions électroniques, et l'identité électronique.
Le but et la finalité est d'aboutir à une collecte effectuée de manière éthique et légale. Et cela passe forcément par ce qui est juridique, le MCDS doit notamment mettre en place un accès sélectif ou « par tranches » au dossier du patient pour limiter les risques de fraude, d'usurpation ou de consultation abusive.

Pilier 2 : Base médicale forte

Nous recommandons la création d'un comité stratégique de données de santé (CSDS) inspiré du modèle français[23] et qui sera rattaché au ministère de la santé et de la protection sociale, qui aura comme objectifs majeurs : qualité, pertinence scientifique et potentiel d'usage des données de santé.
Concernant la garantie de la qualité des données, le comité devrait établir un cadre de qualité robuste pour le MCDS, et cela passerait par la définition de critères de qualité (établir des seuils minimaux de complétude), de cohérence et de validité pour chaque variable, l'adoption de méthodes de contrôle qualité où il faudra recommander des procédures automatisées de détection des anomalies et incohérences, sans négliger le facteur humain essentiel à tout processus via la formation des professionnels en sensibilisant les praticiens et administratifs hospitaliers à l'importance de la qualité du recueil à la source.

Ce comité stratégique de données de santé aurait également la responsabilité de définir les spécifications techniques d'implémentation du MCDS, et devrait suivre un schéma de pilotage de l'implémentation progressive, où il devrait orchestrer le déploiement pratique du MCDS, et ce par l'identification des établissements pilotes en sélectionnant les structures de santé pour tester l'implémentation du socle commun avant le déploiement national, et l'élaboration d'un calendrier de déploiement (établir un plan échelonné tenant compte des capacités techniques et des ressources des établissements). Le comité doit assurer l'évolution continue de ce MCDS, en conduisant une veille sur les standards internationaux émergents, ainsi que le feedback des utilisateurs, pour enrichir ce socle sans compromettre sa stabilité.

Le rôle du comité stratégique dans la création du MCDS est donc à la fois stratégique, technique et opérationnel : il définit la vision, arbitre les choix techniques, produit les outils d'implémentation et pilote le déploiement progressif tout en garantissant qualité et conformité réglementaire en coordination avec les différentes instances du pays (ministère de la Santé, GST, HAS, CNDP). Ce MCDS doit être adapté au

contexte marocain incluant les spécificités locales comme l'Assurance Maladie Obligatoire (AMO), le modèle des structures de soins existantes, et les priorités médicales nationales.

Il ne faudrait pas non plus négliger le rôle des sociétés savantes qui doivent être impliquées pour enrichir le MCDS de variables spécifiques à leur spécialité, valider la pertinence clinique des données collectées, puisqu'elles représentent les organismes de médecins de différentes disciplines, dans le cadre du "*Human Centered Design"* qui vise à intégrer le professionnel de la santé dans le processus d'élaboration des outils liés au MCDS afin d'instaurer un outil familier aux utilisateurs finaux qui sont au contact de la réalité.

Pilier 3 : Gouvernance des relations externes

1. Gouvernance des données partagées avec l'AMO

La maîtrise et la gouvernance des données, en particulier celles transmises aux organismes d'assurance maladie obligatoire (AMO), constituent un enjeu stratégique majeur pour les Groupements Sanitaires Territoriaux. Tout flux de données vers ces organismes doit impérativement respecter le principe de minimisation : seuls les champs strictement nécessaires au traitement des remboursements doivent être transmis.

S'agissant de l'identification du patient, lorsque le système MCDS recourt au numéro de la carte d'identité nationale (CIN) comme identifiant principal, des mesures de sécurité renforcées s'imposent. Cette approche doit être juridiquement justifiée auprès de la Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP) et formalisée par une autorisation explicite de celle-ci, conformément aux dispositions de la loi marocaine 09-08.

2. Standards d'interopérabilité

Pour que le MCDS devienne un véritable catalyseur de transformation numérique au sein des GST, son déploiement doit s'appuyer sur un socle de standards reconnus, tant au niveau international que national.

Standards internationaux

CIM-10 (Classification Internationale des Maladies, 10e révision) est le standard reconnu par l'OMS pour le codage des diagnostics. Elle permet de coder plus de 14 400 diagnostics différents, incluant les maladies, signes, symptômes, lésions traumatiques et causes externes de blessures[24].

Le SNOMED CT (*Systematized Nomenclature of Medicine - Clinical Terms)* constitue la terminologie clinique mondiale la plus complète pour les concepts médicaux. SNOMED CT est particulièrement utile pour les observations cliniques complexes et offre une granularité supérieure permettant la représentation précise de concepts cliniques[25].

Le LOINC (*Logical Observation Identifiers Names and Codes*) est le standard international pour identifier les tests de laboratoire et les observations cliniques. Ce LOINC couvre plus de 20 ans d'évolution et contient maintenant des termes pour les signes vitaux, les mesures radiologiques, les instruments d'évaluation standardisés et les mesures rapportées par les patients[26].
Les variables retenues sont codifiées selon les standards internationaux pour assurer interopérabilité et qualité et chaque élément de donnée doit avoir une source clairement documentée pour garantir sa fiabilité et sa traçabilité au sein de la chaîne de traitement des données.

Standards nationaux

La Classification commune des actes médicaux (CCAM) constitue le standard marocain établi pour identifier les actes professionnels de santé. Pour le contexte marocain, le MCDS doit être aligné avec cette CCAM pour assurer la compatibilité avec les systèmes d'assurance maladie obligatoire (AMO).

3. Portée territoriale du MCDS

L'adoption d'un MCDS basé sur ces éléments garantit un langage de données partagé entre médecins, infirmiers et administrateurs, simplifie l'interopérabilité technique des SI des GST et facilite un système régional unifié pour le suivi des parcours patients et des indicateurs de performance. Cela réduit les actes redondants, erreurs de saisie et examens inutiles, améliorant l'efficience globale du système de santé territorial.

Dans le cadre de la mise en œuvre du Modèle de Socle Minimal de Données Cliniques (MCDS), il est recommandé que l'ensemble des items soit structuré selon des standards nationaux et internationaux d'interopérabilité afin d'assurer la qualité, la traçabilité et l'échange sécurisé des données :

- L'identification du patient doit être réalisée au moyen d'un pseudonyme généré à partir des identifiants internes du système d'information hospitalier. La traçabilité du lien entre identifiant réel et pseudonyme doit être garantie, et les taux d'erreurs de rapprochement (homonymies) doivent être régulièrement évalués, conformément à la loi marocaine 09-08 et aux recommandations de la CNDP, afin de concilier suivi longitudinal et protection des données personnelles.

- Les données démographiques doivent être saisies dans des formats normalisés, notamment le standard ISO 8601 pour les dates et heures, afin de faciliter les calculs de durée, la traçabilité et l'analyse épidémiologique. Les variables telles que le sexe, l'âge et le statut matrimonial doivent être codifiées de manière homogène dans tous les établissements.

- Les données relatives au séjour, la structuration des informations d'admission, d'orientation et de sortie du patient doit suivre un modèle standardisé, en s'appuyant notamment sur les référentiels internationaux tels que HL7-FHIR (*Encounter*), afin de favoriser l'interopérabilité entre structures et niveaux de soins.

- Les diagnostics principaux et associés doivent être codés selon la CIM-10 adoptée au niveau national, afin d'assurer l'harmonisation des pratiques de codage, la comparabilité des données et la production d'indicateurs fiables de morbidité et de gravité.

- Pour les actes médicaux et chirurgicaux, il est recommandé d'intégrer des terminologies normalisées telles que SNOMED-CT ainsi que les nomenclatures nationales (dont la CCAM), permettant la description précise des actes, l'analyse des délais de prise en charge et le suivi de l'activité clinique et opératoire.

- Les examens de biologie, radiologie et constantes cliniques doivent être codés selon des référentiels appropriés, notamment LOINC, et intégrés aux systèmes d'archivage d'imagerie (PACS) afin d'assurer la continuité des informations et de faciliter l'exploitation scientifique et clinique des résultats.

- Les scores cliniques (tels que GCS, OMS, ASA, etc.) doivent être utilisés sous des formes validées et définies de manière standardisée pour permettre l'évaluation de la gravité, du pronostic et l'uniformisation de l'interprétation clinique entre équipes et établissements.

- La déclaration et la codification des événements indésirables et complications doivent se baser sur une terminologie standardisée afin de mesurer la morbidité, la létalité, les taux de réadmission, ainsi que le suivi spécifique des infections nosocomiales et des décès.

- La traçabilité temporelle de chaque événement du parcours patient doit être garantie par l'horodatage systématique selon la norme ISO 8601, permettant l'évaluation des délais hospitaliers, l'analyse du respect des délais critiques et l'optimisation du parcours notamment aux services d'urgences.

Ainsi, l'ensemble de ces éléments permet de disposer d'un modèle de données cliniques structuré, sécurisé et interopérable, facilitant non seulement la prise en charge du patient et la continuité des soins, mais également la production d'indicateurs fiables pour la gestion hospitalière, la recherche et l'amélioration de la qualité des soins au niveau national.

III. Troisième recommandation : Processus de gouvernance standard des données

L'élaboration de recommandations efficaces pour la qualité, la gouvernance, la sécurité et l'interopérabilité des données cliniques constitue une fondation organisationnelle qui repose sur l'établissement d'un préalable essentiel : la définition et la conception.
La gouvernance standard des données commence par une étape cruciale, l'acquisition, qui permet à chaque système de fonctionner comme prévu en ayant suffisamment de données. Ainsi, le stockage de ces données est également indispensable. Considérant la sensibilité de ces données, il est donc primordial d'avoir un système de stockage sécurisé contre tout type d'attaque, qu'elle soit interne ou externe. L'utilisation de ces données est soumise à des conditions basées sur les rôles ou attributs des utilisateurs. La diffusion et l'accès interne de ces données sont contraints à plusieurs règles, de même, le partage et la diffusion externe des données sont soumis à des conditions critiques et fondamentales. Le cycle de vie des données est un point-clé qui finit par l'archivage ou la suppression des données, dans ce chapitre, nous allons déterminer également les étapes de l'archivage/suppression des données.

1. Acquisition

L'acquisition des données dans le domaine médical constitue une étape essentielle, soulevant des enjeux majeurs en matière d'efficacité et de sécurité. En raison de la sensibilité des informations traitées, une protection renforcée des dossiers médicaux confidentiels[27] .

À cet effet, les normes techniques de qualité qui seront mises en œuvre sont les suivantes :

La qualité des données acquises conditionne directement la fiabilité des traitements analytiques et des modèles d'intelligence artificielle qui en dépendent. Parmi les attributs de qualité recensés dans la littérature, trois se distinguent comme prioritaires : La complétude, l'exactitude et la rapidité sont les trois attributs les plus importants parmi un total de 49 attributs de qualité des données[28], car ils assurent que toute donnée critique est présente et disponible en cas de besoin, tout en reflétant l'authenticité clinique de la situation du patient. Sans ce socle, les modèles d'IA produiraient des prédictions non seulement peu fiables, mais potentiellement dangereuses.

Tableau I-1. Critères de qualité des données acquises

Critère	Définition
Complétude	Pourcentage des champs obligatoires non nuls ou vides.
Exactitude/ validité	Pourcentage des valeurs conformes aux règles définies : format, intervalle et système de codage. L'exactitude est étroitement liée à la notion d'ampleur de l'erreur[29].

Cohérence	Pourcentage des enregistrements non contradictoires au sein du système.
Délai	Latence entre la création de la donnée à la source et sa disponibilité dans le système de données électroniques (EDS).
Unicité	Absence d'enregistrements dupliqués pour une même entité patient.

1.1 Interopérabilité

Afin d'assurer une interopérabilité à travers le système, les standards suivants sont recommandés : Conformité FHIR R4, API REST avec authentification OAuth 2.0, support des terminologies SNOMED CT / LOINC.

La saisie des informations dans le Système d'Information Hospitalier (SIH) respecte une attribution précise des tâches basée sur les compétences et la fonction clinique, par conséquent, l'identification des responsables de saisie dans le milieu hospitalier et types de données collectées est fondamentale :

Acteur	Type de données saisies	Responsabilité
Secrétaire médical / Agent d'accueil	Données administratives à l'admission	Enregistrement initial du patient
Infirmier / Infirmier auxiliaire	Paramètres cliniques et constantes v-itales	Mesures et saisies régulières
Médecin / Interne supervisé	Diagnostics, prescriptions, rapports	Validation clinique
Technicien de laboratoire	Résultats de laboratoire et d'imagerie	Saisie et validation technique
Pharmacien hospitalier	Données relatives à la distribution des médicaments	Vérification et enregistrement

La gouvernance des données au sein des Groupements Sanitaires Territoriaux s'étend à l'ensemble des données générées ou reçues, qu'elles émanent des patients, des professionnels de santé ou des systèmes d'information interconnectés. Cette couverture exhaustive implique la collecte, la structuration et la gestion d'un corpus de données hétérogènes, classifiées selon leur nature et détaillées ci-après.

Tableau I-2. Classification des données de santé au sein des GST

Catégorie	Type de Donnée	Exemples
1. Données de soins primaires	Données d'identification	Nom, prénom, date de naissance, numéro d'identification national de santé.
	Données cliniques essentielles	Antécédents médicaux, diagnostics (selon SNOMED CT), traitements et prescriptions, comptes rendus de consultation, allergies.
2. Données issues des soins spécialisés et hospitaliers	Données exploratoires	Résultats de laboratoire (biochimie, hématologie), Comptes rendus d'imagerie (radiologie, tomodensitométrie, IRM), Résultats des tests fonctionnels.
	Données de surveillance hospitalière	Observations infirmières continues, Constantes vitales, Scores cliniques, Comptes rendus opératoires et d'anesthésie.
3. Données pour la recherche et l'innovation *(usage secondaire)*	Données pseudonymisées	Cohortes de patients pour essais cliniques, jeux de données pour l'entraînement de modèles d'intelligence artificielle.
4. Données de gouvernance et de conformité	Données de traçabilité	Journaux d'accès et d'audit, recueils de consentements, historiques de modifications.
	Données de qualité	Indicateurs de performance clinique, métriques de qualité des données, rapports d'incidents et de conformité réglementaire.

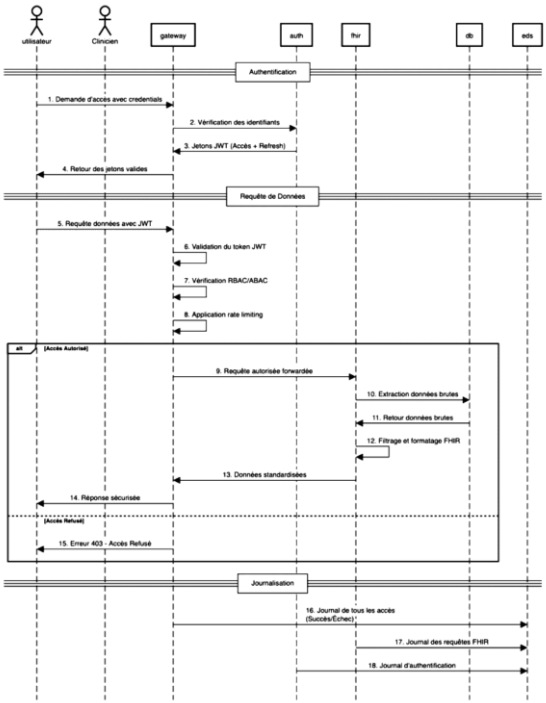
Le Dossier Médical Partagé (DMP) constitue le référentiel central du socle de données cliniques minimales standardisées. Il représente la source de données autorisée pour l'identification des patients et l'accès à leurs données démographiques, allergies, antécédents médicaux, traitements chroniques, comptes rendus d'examens et rapports hospitaliers.

Ces données alimentent l'Entrepôt de Données de Santé (EDS) du GST via des APIs FHIR sécurisées, garantissant ainsi leur consolidation et leur accessibilité auprès des seuls professionnels de santé habilités.

1.2 Flux de travail

Ce processus décrit les étapes standardisées de surveillance, de contrôle et de prise de décision concernant les données de santé GST, de l'acquisition à la destruction. (Annexe. I-1)

Figure I-1. Architecture de circulation des données fondée sur le modèle *Zero Trust*



Note terminologique : API Gateway — Passerelle applicative chargée d'intercepter l'ensemble des requêtes entrantes, de vérifier les droits d'accès et de les acheminer vers le service approprié. **FHIR** *(Fast Healthcare Interoperability Resources)* — Standard international d'interopérabilité pour l'échange structuré des données de santé.

L'authentification est la première étape que chaque acteur devra passer, leur authentification est transférée à la passerelle API où il reçoit des jetons d'accès et des jetons rafraîchit si l'authentification est un succès, puis l'acteur envoie des requêtes qui seront interceptées par la passerelle API qui s'assure de la validité des jetons, de leurs limites et des rôles inscrits dans les jetons, puis la passerelle API transfère la requête

autorisée vers l'API FHIR qui traduit les requêtes en la bonne terminologie et nomenclature puis reçoit les données depuis la base de données et les retourne de manière traduite vers le passerelle API qui envoie une réponse sécurisée vers l'interface des utilisateurs.

L'acquisition sécurisée de données via TLS 1.3 avec chiffrement des API FHIR est un des principaux contrôles qui s'aligne avec les protocoles obligatoires de transfert d'information par le standard ISO 27001 pour la sécurité des communications.

2. Stockage

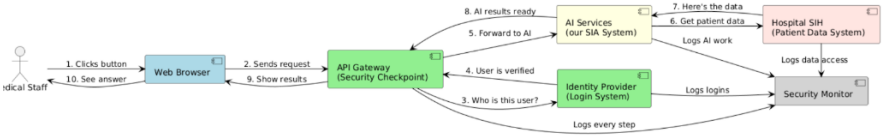


Figure I-2. Stockage des données

Les données cliniques au sein du DMP, qu'elles soient des observations cliniques, des diagnostics, des prescriptions ou des résultats de laboratoires, sont structurées et stockées exclusivement selon le standard international HL7 FHIR R4 ce qui garantit une interopérabilité automatique fondamentale.
Le stockage est aussi garanti en utilisant des *Data Lakes* avec zones brutes / nettoyées / analytiques :

- **Zone brute** — extraction des SIH via FHIR, données sources non modifiées.
- **Zone de nettoyage** — données normalisées et préparées (nettoyage + pseudonymisation + enrichissement).
- **Zone analytique** — où sont stockées les données nettoyées, prêtes pour l'analyse et l'IA.

3. Usage

Lors de la prise en charge d'un patient, le système d'information d'intelligence artificielle (SIA) pourra être utilisé par différents acteurs : l'infirmier pourra l'utiliser pour la saisie des signes vitaux. Le médecin prescripteur pourra entrer le diagnostic (codés avec SNOMED CT), les prescriptions et les notes de procédures, le technicien de laboratoire ou d'imagerie pourra saisir les résultats de laboratoire (codés avec LOINC) et les rapports.

Toute saisie sera soumise à une validation du cadre de santé, afin d'assurer la qualité et la complétude des données au niveau départemental, puis à une validation sémantique par le médecin responsable de l'information médicale, garant de la cohérence clinique des données intégrées dans les entrepôts. Les données saisies seront ensuite transférées vers la base de données via des passerelles API sécurisées, standardisées selon le format HL7 FHIR et codifiées à l'aide des nomenclatures SNOMED CT et LOINC afin de garantir l'interopérabilité. Les données seront pseudonymisées et chiffrées dès leur intégration dans

la base, assurant ainsi leur protection pour tout usage ultérieur de recherche ou d'analyse. Lorsqu'un médecin ou un chercheur souhaite accéder aux données, il adresse une requête à la passerelle API, qui vérifie les jetons d'accès JWT et transmet la requête autorisée à l'API FHIR. Celle-ci interroge la base de données et retourne les informations en fonction de l'identité de l'utilisateur, de ses droits d'accès et des règles de protection applicables, les données pouvant être restituées sous forme pseudonymisée, anonymisée ou identifiante selon le contexte d'usage et les autorisations accordées.

Pour la facturation et le reportage externe en raison de statistiques surveillance de la santé publique ou facturation, le code utilisé sera CIM-11 qui est un code classificateur qui constitue le système de sortie pour les utilisations de données secondaires.

4. Diffusion et accès internes

Comme mentionné, les rôles seront attribués de manière logique suivant les droits d'accès en utilisant une matrice RBAC, il est donc recommandé de séparer les rôles de saisie de données et les rôles de validation de données.
Pour le rôle de saisie de données, l'infirmier pourra saisir les signes vitaux des patients, l'administration des médicaments, etc. Ainsi, le médecin prescripteur ou le médecin interne avec la supervision du médecin prescripteur pourra saisir le diagnostic, les prescriptions, les notes de procédure et les résumés de sortie, la secrétaire médicale pourra saisir les données administratives.
Pour la validation des données, le cadre de santé pourra gérer la qualité des données et leur complétude pour chaque département concerné. Ainsi, le MRIM a l'ultime responsabilité de la validité sémantique et la qualité des données cliniques dans les EDS.

5. Partage et diffusion externes

5.1 Techniques de désidentification

La pseudonymisation empêchera l'identification des patients pour la recherche collaborative en remplaçant certaines informations identificatoires. Elle permet le couplage des données entre plusieurs bases, tout en protégeant l'identité du patient. Cependant, la pseudonymisation n'est pas suffisante car certaines données non anonymisées peuvent suffire pour la réidentification des patients.
Les organisations publiques, en particulier celles utilisant des services cloud, mettent en œuvre diverses techniques de protection des données pour sécuriser les informations personnelles et se conformer à la loi 09-08. L'anonymisation et la pseudonymisation réduisent l'identifiabilité des individus, permettant un traitement ou un partage sûr des données. Le chiffrement garantit que seules les parties autorisées peuvent accéder aux informations sensibles.[30]

5.2 Procédures légales et protocoles sécurisés :

Conformément à la loi 09-08, le partage de données peut reposer sur plusieurs bases légales, notamment le consentement explicite du patient ou l'exécution d'une mission d'intérêt public. Pour les collaborations de recherche, le régime de l'intérêt public est souvent applicable. La gouvernance des accès sera assurée

par une structure tripartite :

- Un comité d'éthique local évaluant la pertinence scientifique et éthique.
- Le Délégué à la Protection des Données (DPO) du GST, émettant un avis conforme sur le respect du cadre légal.
- Le Responsable du traitement (direction du GST) qui, sur la base de ces avis, prend la décision finale et en assume la responsabilité légale.

Cette gouvernance sera formalisée par des procédures écrites approuvées par les instances du GST.

6. Archivage et suppression

Afin de gérer les données selon leur usage et leur criticité opérationnelle, nous recommandons une architecture technique reposant sur une stratification en trois niveaux :

Niveau 1 — Accès immédiat Nous recommandons de réserver ce niveau aux données à fréquence d'usage très élevée : dossiers patients actifs, systèmes d'aide à la décision clinique en temps réel et données d'audit courant. La période de conservation proposée est de **6 mois**.

Niveau 2 — Accès rapide Ce niveau est dédié aux données à fréquence d'usage faible, mobilisées principalement dans le cadre des contrôles qualité et des recherches récurrentes. Nous recommandons une période de conservation de **3 ans**.

Niveau 3 — Accès exceptionnel Nous recommandons de réserver ce niveau aux données à fréquence d'usage très rare, destinées à la recherche à long terme et aux études épidémiologiques. La période de conservation proposée est de **10 ans et au-delà**.

Cette architecture harmonise les coûts de stockage et de performance avec les valeurs cliniques et juridique des données. En réservant le stockage coûteux et rapide aux dossiers actifs (niveau 1), elle optimise les coûts et garantit une performance en temps réel pour les soins critiques. Elle fournit des périodes de rétention claires (six mois, trois ans, 10+ ans) qui simplifie la conformité CNDP et permet une destruction automatisée et légale, réduisant les risques réglementaires. Opérationnellement, elle s'aligne par les flux cliniques des besoins de recherche et d'audit, c'est qui accélère et sécurise l'obtention des informations. Alors que stratégiquement, elle transforme l'archivage d'une contrainte en actif souverain et évolutif pour la recherche nationale. Ce cadre équilibre le besoin immédiat des soins, et la valeur à long terme des données pour l'innovation, assurant la pérennité de l'écosystème numérique de santé marocain.

7. Diagramme du cycle de vie des données:

Le diagramme du cycle de vie des données ci-dessous représente le flux de données commençant par les données du patient (ou toute autre source de données) et les cas d'utilisation des données de tout acteur.

(Annexe I-2).

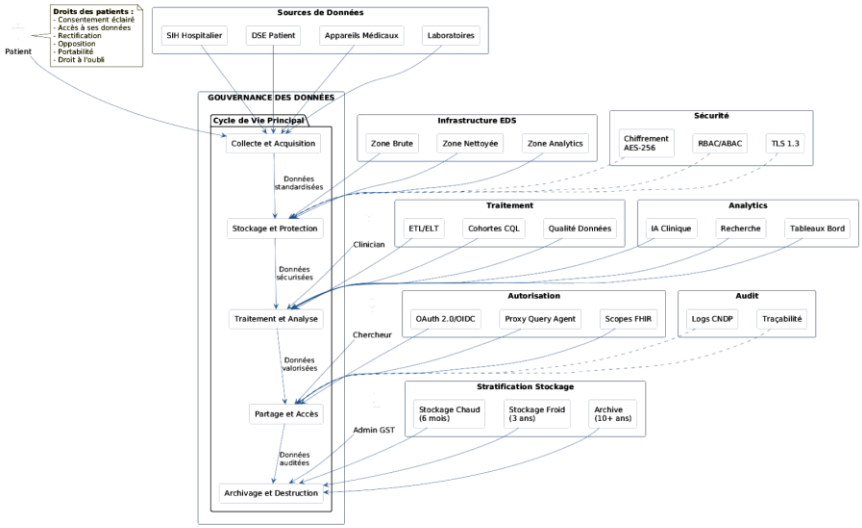


Figure I-3. Modèle recommandé de cycle de vie des données hospitalières

IV. Quatrième recommandation : Renforcement des capacités légales

1. Objectif

La présente recommandation vise à renforcer le cadre juridique applicable aux traitements de données de santé, dans un contexte marqué par la montée en puissance des exploitations algorithmiques à grande échelle. Si la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel encadre les traitements automatisés, y compris lorsqu'ils portent sur des données de santé, elle ne permet pas, en l'état, d'appréhender pleinement certains risques émergents liés aux usages avancés de ces traitements, dont l'intelligence artificielle constitue une forme particulièrement avancée, notamment en matière d'opacité, de biais, de réutilisation secondaire des données et de décisions automatisées à fort impact.
Dans la perspective de la mise en place d'un cadre national de gouvernance des données de santé, notamment au sein des Groupements Sanitaires Territoriaux, le renforcement et l'adaptation de ce cadre juridique apparaissent nécessaires afin d'assurer une exploitation automatisée des données compatible avec les exigences de protection des données personnelles et de la vie privée.

2. Évaluation du cadre légal actuel

La loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel constitue, depuis sa promulgation en 2009, le socle juridique fondamental de la protection des données au Maroc. Conçue selon un principe de neutralité technologique, elle s'applique à tout traitement automatisé de données à caractère personnel, indépendamment des outils techniques mobilisés[31]. À ce titre, les traitements algorithmiques, y compris ceux reposant sur des systèmes d'apprentissage automatique, entrent pleinement dans son champ d'application.

Toutefois, si la loi 09-08 permet d'encadrer juridiquement les traitements automatisés de données en tant que tels, elle demeure insuffisamment outillée pour appréhender certains risques spécifiques induits par les usages contemporains des traitements algorithmiques complexes, en particulier lorsqu'ils portent sur des volumes massifs de données de santé et qu'ils participent à des processus d'aide à la décision ou de pilotage du système de soins. Ces limites ne tiennent pas à une absence de règles applicables, mais à un décalage fonctionnel entre un cadre normatif conçu pour des traitements essentiellement déterministes et centralisés, et des pratiques actuelles caractérisées par la complexité croissante des modèles algorithmiques, la réutilisation secondaire et continue des données, l'opacité fonctionnelle de certains traitements, et l'impact potentiel des décisions automatisées sur les droits et la prise en charge des patients.

Dans le domaine de la santé, ces enjeux prennent une acuité particulière en raison de la sensibilité des données concernées, de la dépendance croissante aux outils numériques et de la portée collective des décisions fondées sur l'exploitation automatisée des données. Il en résulte une insécurité juridique relative, non pas quant à l'applicabilité de la loi, mais quant à sa capacité à prévenir et encadrer efficacement les

risques systémiques associés à ces nouveaux usages.

3. Renforcement du cadre légal

3.1 Adaptation de la loi n° 09-08 aux enjeux des traitements algorithmiques automatisés :

Bien que la CNDP rappelle que les traitements impliquant des données à caractère personnel, y compris ceux utilisés par l'intelligence artificielle, demeurent soumis à la loi n° 09-08[32], ce cadre révèle aujourd'hui ses limites face aux risques engendrés par la complexité des systèmes de traitements automatisés, dont fait partie l'IA. Promulguée en 2009, cette législation est jugée moins opérante dans la mesure où elle s'avère obsolète face à l'expansion massive de la capacité à utiliser les données (*big data*) et aux modèles d'apprentissage automatique actuels, dont l'essor est continu. Dès lors, la révision de cette loi est devenue une condition *sine qua non* à la réussite du cadre de gouvernance des données de santé au sein des GST. Cet ajustement permettra de sécuriser l'exploitation automatisée des données des patients tout en garantissant un haut niveau de protection des informations personnelles.

L'impératif de révision ainsi identifié trouve un écho particulier dans les orientations stratégiques nationales et les engagements internationaux du Royaume du Maroc. Le Conseil Économique, Social et Environnemental a, dans cette perspective, souligné l'urgence d'une mise en conformité de la loi 09-08 afin qu'elle puisse intégrer valablement les exigences liées aux données utilisées et générées par l'IA[33]. Cette mutation ne relève pas d'une simple mise à jour technique, mais d'une exigence de congruence avec les standards mondiaux, à l'instar des recommandations de l'Organisation des Nations unies pour l'éducation, la science et la culture sur l'éthique de l'intelligence artificielle. En s'engageant dès 2022 à mettre en œuvre ces principes[34], le Maroc a tracé la voie vers un nouveau paradigme de régulation où la transparence, l'explicabilité, l'équité, l'inclusion ou encore la non-discrimination ne sont plus des options, mais des composantes intrinsèques de la licéité des traitements automatisés.

L'analyse de l'évolution des pratiques juridiques étrangères confirme cette transition vers un encadrement plus granulaire, capable de saisir la substance même des risques algorithmiques. L'expérience française, notamment à travers la loi JOP de 2024[35], illustre cette tendance par la création d'un régime spécifique aux traitements algorithmiques à fort impact, imposant des garanties de contrôle humain et de limitation stricte des finalités. Dans la même logique, les approches canadienne[36] et européenne[37] privilégient désormais une régulation modulée par le niveau de risque, imposant des obligations de diligence renforcées pour les systèmes dits « à haut risque ». Ces modèles comparatifs démontrent qu'un cadre moderne doit savoir s'extraire de la seule protection de la donnée pour s'intéresser à la loyauté de l'algorithme qui la traite, particulièrement lorsque ce dernier influe sur les droits fondamentaux des individus.

Dès lors, l'adaptation du cadre législatif marocain doit être envisagée comme le levier de sécurisation du futur écosystème de santé territoriale. Au sein des GST, où la massification des données de santé devient un outil de pilotage clinique et administratif, l'introduction de mécanismes dédiés à la gestion des biais et

à la responsabilité algorithmique est primordiale. Une réforme ciblée de la loi 09-08 permettrait ainsi d'ériger les principes de transparence et de pertinence des données d'entraînement en normes opposables, évitant que l'automatisation des soins ne se traduise par une dépersonnalisation de la prise en charge ou une fragilisation du secret médical.

In fine, cette évolution législative devient l'épine dorsale d'une souveraineté numérique sanitaire. En dotant le pays d'un arsenal juridique capable d'appréhender la complexité des traitements automatisés, le Maroc s'assure une transition vers la santé numérique qui soit à la fois performante et protectrice. Loin de bouleverser l'architecture initiale de la protection des données, cette réforme ciblée viendrait parachever le dispositif existant, garantissant que l'innovation technologique demeure subordonnée aux impératifs éthiques et aux droits des patients, conditions essentielles d'une confiance durable dans le progrès médical.

3.2 Promulgation d'une loi encadrant le *big data* :

Le terme *big data* est régulièrement mobilisé, sans pour autant être clairement défini[38]. En pratique, il renvoie à l'ensemble des données caractérisées par un volume extrêmement important, une grande variété de formats et une vitesse de production et de traitement très élevée. Ainsi, conformément à l'étude annuelle 2014 du Conseil d'État français, le *big data* désigne non seulement l'expansion du volume des données mais aussi celle de la capacité à les utiliser et il dépend généralement de cinq facteurs à savoir le volume des données traitées, leur variété, la vélocité et la capacité des applications à les traiter notamment en temps réel, leur véracité et enfin la valeur qui peut en être tirée[39]. Malgré ces efforts de conceptualisation, le *big data* n'a toujours pas fait l'objet d'une définition formelle dans le droit positif marocain, ce qui crée un vide juridique et rend difficile l'application des mécanismes existants de protection des données personnelles, notamment dans des secteurs fortement consommateurs de données comme la santé.

Dans ses pratiques, l'industrie de la santé manifeste un intérêt majeur pour l'exploitation du *big data* puisqu'il s'appuie fortement sur les données médicales dans ses processus décisionnels[40]. Ces données se présentent sous des formes multiples, souvent variées, non structurées et complexes, que les systèmes de gestion de bases de données traditionnels ne peuvent traiter efficacement[41]. Ce type de traitement semble, à première vue, échapper au champ d'application de la loi 09-08. Pourtant, même lorsque les données massives ne sont pas directement identifiantes, elles peuvent tout de même porter atteinte aux droits des personnes. Cette problématique est d'autant plus accentuée que les systèmes de traitements automatisés et notamment l'IA, de plus en plus utilisés dans le domaine médical, reposent eux-mêmes sur l'exploitation de vastes ensembles de données afin d'améliorer leurs performances analytiques et prédictives.

En effet, l'exploitation de larges volumes de données médicales peut permettre d'identifier ou de réidentifier indirectement des personnes, notamment par le croisement de sources multiples ou l'analyse de comportements. Les risques sont accrus lorsque les données sont traitées par des algorithmes avancés capables de reconstituer des identités à partir d'indices fragmentaires. Même lorsque les données sont anonymisées, différents travaux ont montré que des données considérées anonymes pouvaient être ré-identifiables par ces procédés d'identification indirecte[42]. Par ailleurs, la logique même du *big data*, fondée sur une collecte extensive préalable et une détermination secondaire des usages, se heurte directement aux

principes de finalité, de proportionnalité et de pertinence consacrés par la loi 09-08. L'intégration croissante de l'IA dans ces traitements renforce ces tensions, puisque la performance des modèles repose souvent sur l'accumulation et le croisement de données, augmentant mécaniquement les possibilités d'atteinte à la vie privée. L'ensemble de ces éléments démontre que les mécanismes actuels sont insuffisants pour encadrer les traitements massifs et complexes et pour prévenir efficacement les risques inhérents au *big data*.

Face à ces constats, la promulgation d'une loi spécifique dédiée au *big data* apparaît comme la voie la plus pertinente. En effet, chercher à intégrer l'ensemble des enjeux liés au *big data* dans la loi 09-08 impliquerait une refonte profonde de ses concepts fondateurs, notamment la finalité, la proportionnalité, les données à caractère personnel[43] ou encore les logiques de consentement, au risque de déséquilibrer l'architecture juridique existante. À l'inverse, une loi autonome permettrait de poser des règles adaptées aux traitements massifs, évolutifs et fondés sur des données hétérogènes, tout en maintenant la cohérence de la loi actuelle sur la protection des personnes physiques à l'égard du traitement des données personnelles.

Un tel cadre devient d'autant plus indispensable que l'essor des technologies des traitements automatisés dépend directement de la disponibilité de données massives, ce qui impose de concilier développement technologique, exigences opérationnelles en santé, et respect des droits fondamentaux. Cette conciliation est d'autant plus impérative que la recherche scientifique et la protection de la vie privée figurent parmi les droits expressément garantis par la Constitution marocaine de 2011. Une loi dédiée au *big data* constituerait ainsi un instrument essentiel pour assurer à la fois innovation, sécurité juridique et protection effective des individus.

V. Cinquième recommandation : Renforcement des capacités institutionnelle

1. Objectif

L'objectif principal de la présente recommandation est de mettre en valeur quelques mécanismes ayant pour objectif le renforcement des capacités des institutions marocaines existantes. Ce renforcement a pour finalité de promouvoir le rôle de ces institutions afin de créer et de garantir une confiance citoyenne collective tout au long du processus de modernisation et du développement du secteur sanitaire, en s'assurant que tout traitement impliquant les données des patients n'est effectué que sous total respect de la législation et des normes en vigueur, et de celles potentiellement promulguées.

2. Évaluation des capacités institutionnelles

Dans un contexte de transformation numérique, portée par les stratégies nationales de digitalisation des services publics, et par l'intensification des débats sur le déploiement de l'IA, la protection de la vie privée des personnes, en l'occurrence leurs données, est devenue un enjeu majeur auquel le Maroc devra faire face en se dotant d'une structure institutionnelle solide.

C'est dans ce sens que s'est instituée la CNDP. Instaurée par la loi 09-08, la CNDP a pour mission phare d'assurer le contrôle des pratiques des acteurs bien publics que privés en matière de traitement des données à caractère personnel [44].

Aux fins d'accomplir cette mission, la CNDP s'est dotée par le biais de la loi 09-08 d'un champ étendu de rôles et de pouvoirs[45]. Entre consultation, sensibilisation, information, veille juridique, la protection reste l'axe majeur et central autour duquel s'articule la majorité des pouvoirs procurés à la CNDP. À ce titre, la commission reçoit les plaintes des individus estimant être lésés de la publication d'un traitement de données, les instruit et ordonne soit la publication des rectificatifs soit la saisie du procureur du Roi aux fins de poursuite, elle procède également aux rectifications justifiées demandées par l'intéressé lorsque le responsable du traitement refuse d'y procéder. D'autant plus, la commission dispose du pouvoir d'ordonner le verrouillage, l'effacement ou la destruction des données et d'interdire, provisoirement ou définitivement le traitement des données à caractère personnel.

Bien que cette consécration de pouvoirs reflète une volonté claire et ferme de protéger les données personnelles, et d'aligner le cadre juridique national sur les expériences et standards internationaux, leur efficacité est loin d'être satisfaisante à plusieurs échelles, surtout face à l'expansion fulgurante de l'IA[46]. C'est dans ce sens que le renforcement du rôle de la CNDP, se présente comme un levier majeur pour une transformation digitale responsable et surtout sécurisée[47].

À côté de la CNDP, le Maroc a solidifié sa base institutionnelle par la mise en place de l'Institut Marocaine de la Normalisation (IMANOR) par le biais de la loi n°12-06, ainsi que le conseil supérieur, de certification et d'accréditation (CSNCA)[48]. L'introduction de ces organes à l'arsenal juridique marocain était portée par une vision stratégique motivée par la mise du cadre normatif marocain au rang des normes internationales

dans différents domaines. Dans ce cadre, la loi n°12-06 a doté ces organes d'une étendue de pouvoirs et de missions axés essentiellement autour de la normalisation qui consiste en l'élaboration, la publication et la mise en application de documents de référence dits normes[49]. La certification, permettant d'attester après vérification la conformité aux normes homologuées[50] et finalement l'accréditation.

Dans l'ampleur du contexte technologique actuel et face à la montée en puissance de ses enjeux, en l'occurrence la protection des données à caractère personnel, la consolidation du socle institutionnel est devenue imposante pour la mise en place d'un cadre robuste pour la sécurité et la qualité des données, aligné sur les exigences internationales. Pour cette fin, l'IMANOR et la CNDP ont conclu une convention de partenariat en juillet 2021 qui s'étale sur quatre ans renouvelables[51], dont la concrétisation s'impose plus que jamais, dans l'essor de l'IA dans des domaines stratégiques, en l'occurrence, la santé.

3. Mécanismes de renforcement

3.1 Renforcement du rôle de sensibilisation et d'information de la CNDP

En réponse à la multitude des critiques relevées à propos de l'insuffisance des efforts de la CNDP dans l'information et la sensibilisation [52], il est fortement recommandé de renforcer son rôle en développant une stratégie nationale de sensibilisation continue visant la protection des données sensibles. Une étape indispensable pour la création d'un climat de confiance numérique collective, et un levier primordial pour la mise en place d'un État digital et moderne aux termes du Conseil économique, social et environnemental. Cette stratégie devrait s'inscrire dans une démarche de long terme et continue ciblant l'ensemble des acteurs impliqués[53].

À l'instar de l'expérience de la Commission Nationale de l'Informatique et des Libertés (CNIL) en France, la CNDP pourrait mettre en place un programme structuré d'actions de proximité, (ateliers, interventions en milieu scolaire, séances d'information dans les administrations, des campagnes itinérantes dans les espaces publics privilégiant des messages simplifiés en langue locale), permettant à chacun de comprendre les enjeux de la vie privée à l'ère du numérique et de maîtriser l'usage de ses données personnelles. Un tel dispositif contribuerait directement à l'instauration d'un État digital fiable et responsable, fondé sur la transparence, la sécurité et la confiance[54].

3.2 Renforcement de la coopération institutionnelle pour la gouvernance des données de santé

La réforme que connaît actuellement le secteur sanitaire, est le terrain propice pour concrétiser le partenariat institutionnel entre la CNDP et l'IMANOR et ce à plusieurs échelles. Grâce à l'expertise et le mandat légal conféré à la CNDP à propos du contrôle de la protection des données à caractère personnel, et la mission de l'IMANOR en tant qu'institution de normalisation, l'alliance de cette double expertise institutionnelle paraît stratégique bien que pivot pour l'accompagnement de la digitalisation du domaine sanitaire de façon fiable et sécurisée centrée sur la protection du citoyen, notamment ses données.

Dès lors, il conviendrait prioritairement d'élaborer des référentiels normatifs sur la protection des données à caractère personnel au sein des GST. Ces référentiels élaborés sous l'égide de l'IMANOR et orchestrés par la compétence de la CNDP, permettront de transposer les dispositions légales définies par la loi 09-08, et des normes internationales portés par l'Organisation internationale de normalisation (ISO), en l'occurrence, la norme ISO/IEC 27701 relative à la sécurité d'information, cybersécurité et protection de la vie privée[55] en exigences techniques et opérationnelles opposables au sein des GST. Cette alliance institutionnelle devrait également se présenter comme occasion pour la normalisation d'audits rigoureux pour la surveillance régulière de l'intégrité du processus lié au traitement des données sensibles des patients, et de même prévoir les critères de certification des établissements au sein des GST afin de promouvoir une confiance citoyenne collective.

3.3 Renforcement des mécanismes d'accompagnement professionne

Le métier du DPO a pris de l'ampleur sur la scène internationale, notamment sous l'impulsion du règlement général sur la protection des données (RGPD), qui prévoit dans son article 37 les modalités de désignation du DPO, aussi l'article 38 et 39 qui clarifient respectivement les fonctions et les missions du délégué à la protection des données[56]. Bien que son statut reste légalement indéfini, le président de la CNDP en reste pleinement conscient[57]. Par la suite, il est recommandé de prime abord de définir le statut légal du DPO, ses fonctions, missions et obligations, en l'occurrence au sein des GST afin d'éviter le flou juridique sur un acteur dont l'émergence est vivement recommandée. Au-delà de cette reconnaissance légale et formelle, la CNDP devrait déployer une véritable feuille de route nationale destinée à encadrer l'émergence de ce nouveau corps de métier. Ce dispositif stratégique viserait à catalyser l'intégration de cet acteur pivot au sein des structures publiques, tout en garantissant sa montée en compétence.

2.4 Renforcement du pouvoir répressif

Le cadre légal actuel relatif à la protection des données à caractère personnel prévoit un dispositif répressif assez lourd et de gravité graduelle, en cas de violation des normes de traitement légalement imposées, allant de sanctions administratives à caractère disciplinaire[58] confiées à la CNDP à des sanctions pénales (amendes et emprisonnement). Or, la loi ne dote pas la CNDP d'un pouvoir répressif direct, chose qui limite significativement l'impact immédiat du contrôle qu'elle exerce et l'efficacité du dispositif répressif.

A titre de comparaison, la puissance dissuasive du système européen repose en grande partie sur le pouvoir de sanction octroyé par le Règlement Générale sur la Protection des Données (RGPD) aux Autorités de Protection des Données (APD), qui leur confère la possibilité d'infliger des sanctions qui revêtent une forme pécuniaire significative[59].

Dans ce contexte une mise à niveau du cadre légal est nécessaire, et la préparation à la révision de la loi 09-08 devrait être à pied ferme afin de prévoir un véritable pouvoir de sanction pécuniaire directe au profit de la CNDP[60], aligné aux standards internationaux, afin de garantir une dissuasion effective, une réactivité accrue détachée de l'aspect procédural et un renforcement tangible de la protection des droits des citoyens.

VI. Sixième recommandation : Échange et interopérabilité des données

1. Standards d'interopérabilité

Dans l'objectif d'assurer une interopérabilité sécurisée, durable et efficace entre les différents services et composants du système (SIH et EDS), il est nécessaire d'adopter une architecture reposant sur des standards techniques spécifiques.
Les principaux standards techniques recommandés pour assurer l'interopérabilité sécurisée des systèmes d'information de santé sont présentés dans le tableau ci-dessous.

Tableau I-3. Standards d'interopérabilité, de sécurité et de traçabilité des données de santé

Domaine	Standard	Justification technique
Échange de données	HL7 FHIR R4	API RESTful moderne, idéale pour l'intégration et l'IA
Sécurité	OAuth 2.0 / OIDC	Gestion granulaire et sécurisée des accès
Transport	TLS 1.3	Chiffrement robuste des données en transit
Audit	FHIR Provenance	Traçabilité des accès pour la conformité
Requêtes	CQL (Clinical Quality Language)	Logique clinique portable et maintenable

2. Architecture des données

A. Principes directeurs

- Patient-Centricité: Les données sont organisées autour du Patient FHIR comme entité centrale.
- Couches de sémantique : Il y a une séparation claire entre les données brutes, standardisées, et enrichies.
- Gouvernance intégrée : L'architecture inclut des métadonnées, la traçabilité (Provenance FHIR) et le cycle de vie (rétention, archivage) dès la conception.

B. Modèles de données logiques

- Standard : HL7 FHIR R4 comme modèle canonique.
- Profils : On utilise des Profils d'Implementation (IG) nationaux pour adapter les ressources FHIR aux besoins du Maroc (p. ex., PatientMaroc, ObservationSignesVitauxMaroc).

- Référentiels terminologiques :
- SNOMED CT International : Pour les diagnostics et les procédures.
- LOINC : Pour les observations de laboratoire.
- UCUM : Pour les unités de mesure.
- Code National des Actes (CCAM équivalent marocain) : Pour la facturation.

3. Gouvernance des flux — Principe *Zero Trust*

Pour garantir une sécurité maximale, moins de violations, de piratages et d'attaques de cybersécurité, nous utiliserons le principe *Zero Trust*, qui encourage les développeurs à considérer les attaques non pas comme une possibilité mais comme une promesse. Leur travail consiste donc à les rendre moins nombreuses, plus maintenables et plus faciles à suivre/détecter, ce qui implique que les développeurs ne doivent « jamais faire confiance ; vérifiez toujours ». Le principe fonctionne en empilant plusieurs couches de sécurité.

VII. Septième recommandation : Gouvernance et opérationnalisation au niveau des GST

1. Structures locales

Malgré les avancées introduites par la Stratégie Nationale de Digitalisation de la Santé et par le chantier de réforme encadré par la loi-cadre 06-22, les fonctions de gouvernance numérique au sein du ministère restent marquées par une forte centralisation technique et une limitation des capacités opérationnelles. La DIM, structure du ministère, assume simultanément l'élaboration du schéma directeur, et apporte son appui technique en matière d'informatisation aux services centraux et aux services extérieurs [61]. Or, l'extension rapide des infrastructures numériques, la création des GST et la transcendance attendue des systèmes d'information régionaux créent une pression institutionnelle que les dispositifs actuels ne permettent plus d'absorber.

La mise en œuvre des systèmes d'information territoriaux progresse parallèlement avec la création des GST, chacun disposant désormais d'une DSI comme le suppose le modèle de Tanger-Tétouan-Al Hoceima[62]. Toutefois, cette décentralisation fonctionnelle révèle d'importantes disparités entre les régions : hétérogénéité des architectures, absence de standards communs, dépendance aux prestataires externes, insuffisance de contrôle sur la qualité des données et absence d'un mécanisme formalisé de coordination verticale entre le niveau central et les GST [63].

La DIM, rattachée au MSPS, élabore le schéma directeur national et appuie les services centraux et extérieurs. Cependant, ses responsabilités historiques ne couvrent ni les enjeux de gouvernance des données de santé, ni la supervision de l'interopérabilité, ni la régulation de l'usage secondaire des données, ni même des exigences en matière d'audit, traçabilité et cyber sécurité ; désormais essentiels dans un système de santé structuré autour des GST.

I. Analyse du mécanisme institutionnel

La réforme 06-22 repose sur une décentralisation fonctionnelle importante : les GST deviendront responsables de la mise en œuvre locale des systèmes d'information et de la qualité des données produites. Toutefois, aucun mécanisme institutionnel ne formalise aujourd'hui la coordination verticale entre La DIM au niveau central qui est responsable de la stratégie, des normes et du pilotage et des futurs services numériques des GST niveau territorial, responsables de l'exécution, de la supervision et de la conformité.

Cette absence de liaison organique produit trois risques organisationnels :
1) Fragmentation des systèmes et divergence des pratiques [64].
2) Dépendance excessive au niveau central, qui freine la transformation
3) Absence de responsabilité clairement définie pour la gouvernance des données.

Ainsi la DIM définit les priorités nationales mais n'a pas d'autorité fonctionnelle explicite sur les DSI-

GST, qui opèrent les systèmes régionaux mais ne disposent pas d'un cadre national contraignant pour harmoniser leurs pratiques. Sans mécanismes formalisés, la transition numérique risque de reproduire le modèle fragmenté du passé, incompatible avec les exigences de la réforme 06-22.

II. Instrument de politique publique

Cette entité, à savoir la DIM, est recommandée comme organe de pilotage local, à travers la DSI, de la gouvernance des données de santé. Elle assurerait la coordination entre les hôpitaux, laboratoires, et structures de soins primaires, et garantirait la conformité juridique et technique des traitements numériques. Cette recommandation vise à assurer l'autonomie des structures territoriales sans pour autant créer de nouvelles structures.

À titre de comparaison, en France, le *Health Data Hub* a été institué pour piloter l'accès et la réutilisation des données de santé, et dispose de référentiels clairs de gouvernance, ce qui illustre l'intérêt de la mise en place d'une DIM dédiée à la gouvernance des données de santé [65].

Ainsi, il est recommandé que la DIM soit chargée de superviser et harmoniser l'action des DSI affiliées aux GST, Elle traduirait les orientations du MSPS en plans d'action régionaux à travers les DSI-GST, tout en garantissant la conformité, la qualité et la sécurité des pratiques numériques.

L'instrument recommandé est la formalisation d'un cadre national de gouvernance des données territorialisées, reposant sur Deux fonctions spécialisées intégrées au sein de la DIM, chargées de superviser et harmoniser l'action des DSI-GST, sans pour autant créer de nouvelles structures.

A. Fonction nationale de gouvernance des données d'architecture, d'interopérabilité et coordination territoriale avec appui aux GST (DIM)

Leur mandat s'articule autour de six objectifs **:**

1) Le Déploiement du cadre national de gouvernance des données dans les établissements sanitaires conformément aux référentiels de la CNDP et aux directives du MSPS.

2) La coordination institutionnelle entre les structures locales et les directions centrales est recommandée afin de minimiser et d'écarter l'hétérogénéité technologique des SIH. A ce titre, ces structures veilleront à la cohérence technologique et à l'homogénéité des solutions déployées ainsi qu'à l'intégration progressive des SIH régionaux.

Dans une logique de compatibilité fonctionnelle et technique des plateformes locales avec l'entrepôt national des données de santé, cette démarche vise à faire émerger un écosystème numérique unifié, où chaque établissement contribue à la fiabilité, la sécurité et la valeur clinique de la donnée.

3) La cohérence des flux d'information et l'interopérabilité (HL7 FHIR) des systèmes et élaborer les

référentiels nationaux de qualité, sécurité et traçabilité des données. Et garantir l'alignement de chaque projet numérique sur les standards nationaux, notamment le Socle des données et le *MPI*, tout en tenant compte des spécificités territoriales.

4) La Garantie de la conformité au cadre réglementaire de la protection des données personnelles (loi 09-08) et aux standards internationaux de sécurité numérique [66].

5) Le maintien du registre national des traitements et des accès en intégrant la dimension qualité, sécurité et éthique des usages, et réguler les accès et l'usage secondaire des données, en coordination avec la CNDP sous la supervision du MSPS [67].

6) Le Développement des compétences et culture numérique :
Ces structures auront un rôle d'appui et de formation. Elles organiseront, avec le soutien du MSPS et du MESRSI, des programmes de montée en compétence pour les cadres médicaux, administratifs et techniques, portant sur la gouvernance, la cyber sécurité et l'éthique du numérique en santé [68]. Cette approche rejoint les orientations de la Banque mondiale, qui considère le renforcement des capacités institutionnelles comme une condition essentielle à la durabilité des réformes numériques en santé [69]. Elles représenteront, à l'échelle territoriale, la déclinaison directe du MSPS, dans une logique de subsidiarité et de cohérence institutionnelle. En ce qui concerne les DSI-GST, il convient d'appliquer rigoureusement les protocoles en vigueur. Ils doivent également assurer la remontée des audits, des incidents ainsi que des rapports de conformité.

B. Fonction nationale d'audit : composition et positionnement institutionnel (DIM)

La DIM assure une fonction nationale d'audit des systèmes d'information hospitaliers, en veillant à la conformité, à la sécurité et à l'efficacité des dispositifs numériques au niveau territorial. Ces audits seraient réalisés par un comité régional d'audit, composé de représentants clés des différents acteurs de la gouvernance numérique nommés par la DIM. Ces audits seraient conduits à période régulière.

L'audit reste l'une des missions primordiales de la DIM [70], cependant un flou régit la manière dont il sera exécuté, c'est dans ce contexte là qu'on recommande cette mise en œuvre :

1) Pré-audit, planification

Cette étape consistera à identifier des GST concernés et à définir les indicateurs clés, notamment l'utilisation du système, la qualité des données, le respect des procédures et la sécurité informatique. Les équipes locales seront informées et les outils nécessaires préparés, tels que les checklists, questionnaires et extraits de données.

2) L'audit sur site ou à distance :

Sur site : inspection du matériel, formation et interviews du personnel, vérification de l'usage réel du système.
À distance : Analyse des données extraites et leur comparaison aux standards définis.

3) Analyse et recommandations :

La DIM identifie les écarts entre la pratique et les standards, propose des actions correctives prioritaires comme la publication de guides techniques obligatoires pour les GST et prépare un rapport détaillé à soumettre au MSPS.

4) Suivi Post-audit :

La planification de mini-audits pour vérifier la mise en œuvre des recommandations, ainsi que le maintien d'un tableau de bord centralisé permettant de suivre les progrès et les corrections appliquées dans tous les GST.
La documentation associée comprend les checklists d'audit, les formulaires standardisés pour les rapports trimestriels et annuels, et le tableau de bord centralisé pour un suivi global efficace.

III. Articulation hiérarchique et coordination

L'extension du mandat des DIM vise à rapprocher la décision publique du terrain et à faire de la donnée un outil de pilotage, de redevabilité et de confiance. En intégrant la DSI-GST sous l'autorité de la DIM dans le dispositif de gouvernance régionale, le Maroc place la qualité et la sécurité des soins au cœur de la transformation numérique. Cette structure permettra de renforcer la cohérence interinstitutionnelle, de fluidifier la communication entre les acteurs et d'accélérer la mise en œuvre des politiques publiques. Elle constituera, à terme, le socle d'une gouvernance sanitaire distribuée, où les régions deviennent de véritables centres de pilotage et d'innovation institutionnelle. Ainsi, la réforme numérique s'enracine dans une dynamique de souveraineté, d'équité et de durabilité, conformément aux standards de l'OMS [71].

Enfin, La coordination DIM DSI-GST permettra d'assurer une gouvernance numérique territorialisée, réactive et conforme aux standards internationaux. Qui instaurera un modèle de responsabilité partagée entre le niveau central et les territoires, favorisant la transparence, la sécurité et la performance institutionnelle du système de santé.

IV. Impact attendu

La DSI-GST permettra de territorialiser la gouvernance des données de santé, de renforcer la coordination interinstitutionnelle et d'assurer la conformité éthique et technique des systèmes régionaux. En associant la DIM à la supervision des pratiques locales, le dispositif consolide la qualité des soins, la sécurité des données et la redevabilité institutionnelle.

2. Procédures opérationnelles standardisées (SOP)

Les procédures opérationnelles standardisées *(Standard Operating Procedures – SOP)* constituent un instrument central de la gouvernance publique hospitalière dans un contexte de transformation numérique accélérée. Elles traduisent les orientations stratégiques et les exigences réglementaires en règles opérationnelles claires, opposables et vérifiables, applicables de manière homogène à l'ensemble des structures du Groupement Sanitaire Territorial (GST)[72].

Dans le champ de l'intelligence artificielle en santé, les SOP remplissent une double fonction :

- Fonction de sécurisation, en encadrant les usages, les responsabilités et les risques.

- Fonction de pilotage, en permettant le suivi, l'évaluation et l'amélioration continue des pratiques.

Elles constituent ainsi un levier structurant pour l'instauration d'une culture institutionnelle de responsabilité, de transparence et de conformité, sans freiner l'innovation ni la modernisation des services de santé.

SOP n°1 : Signalement et gestion des incidents et risques

Nous recommandons, sous la tutelle du Ministère de la Santé et de la Protection Sociale (MSPS) et en coordination avec les GST, la mise en place d'un dispositif institutionnel unifié de signalement, d'analyse et de traitement des incidents et situations à risque liés aux activités numériques, aux systèmes d'information et à l'usage de l'intelligence artificielle. Ce dispositif s'inscrit dans une logique de prévention des risques systémiques et d'amélioration continue de la qualité des soins, en cohérence avec les standards internationaux de gestion des risques opérationnels[73].

Champ d'application :

Ce dispositif s'applique à l'ensemble des entités relevant du GST : directions hospitalières, structures cliniques et médico-techniques, directions des systèmes d'information, cellules qualité et sécurité, ainsi que les partenaires engagés dans des projets numériques ou de recherche clinique, sous la supervision des autorités de tutelle compétententes[74].

Gouvernance et responsabilités

La supervision stratégique du dispositif incombe au GST, qui assure la production d'un reporting institutionnel consolidé à destination du MSPS[75]. MSPS. Les chefs de service sont responsables de l'animation locale du dispositif et de la sensibilisation continue de leurs équipes. L'ensemble du personnel hospitalier dispose du droit et du devoir de signaler toute situation à risque, dans un cadre explicitement non punitif, favorisant la transparence et la confiance institutionnelle.

Dispositif opérationnel :

Le processus de gestion des incidents repose sur une déclaration normalisée, une analyse graduée de la gravité et de l'impact, l'élaboration de plans d'action correctifs clairement attribués et un suivi documenté jusqu'à la clôture formelle des incidents, conformément aux exigences de traçabilité et de redevabilité[76].

Pilotage et amélioration continue :

Il est recommandé que les données consolidées issues du dispositif de signalement alimentent un tableau de bord institutionnel du GST, permettant d'orienter les décisions stratégiques, de renforcer la coordination avec la CNDP en cas d'incidents impliquant des données personnelles, et de consolider durablement une culture de sécurité numérique au sein des établissements de santé.

SOP n°2 : Évaluation et maîtrise des risques numériques

Finalité :
La structuration d'une méthodologie homogène d'identification, d'analyse et de traitement des risques numériques constitue un levier central de la gouvernance du GST. Cette méthodologie vise à concilier l'innovation technologique, la sécurité des systèmes d'information hospitaliers et la conformité au cadre juridique national, notamment aux dispositions de la loi n°09-08 relative à la protection des données à caractère personnel, en articulation avec les missions de la CNDP[77].

Périmètre :
Cette méthodologie couvre l'ensemble des systèmes numériques hospitaliers relevant du GST, incluant les plateformes de données de santé, les outils d'intelligence artificielle à usage clinique, les dispositifs d'interopérabilité entre établissements, ainsi que les mécanismes de gestion des identités et des accès, afin de garantir une approche globale et cohérente des risques numériques[78].

Principes de référence :
L'évaluation et la maîtrise des risques numériques reposent sur des principes structurants d'anticipation et de prévention des menaces techniques, juridiques et éthiques, de proportionnalité des mesures de contrôle au regard de la gravité et de la probabilité des impacts, de responsabilité partagée entre les acteurs techniques, cliniques et institutionnels, ainsi que de traçabilité et de documentation systématiques de l'ensemble du processus.

Cycle de gestion des risques :
Le dispositif s'appuie sur un registre des risques numériques régulièrement mis à jour, assorti d'une analyse structurée des impacts potentiels sur la sécurité des soins, la continuité des services et la protection des données. Les modalités de traitement des risques distinguent explicitement les options d'évitement, de réduction, de transfert ou d'acceptation, et font l'objet d'un suivi formalisé à l'échelle du GST.

Indicateurs de pilotage :
Des indicateurs synthétiques et harmonisés permettent d'évaluer la performance du dispositif de gestion des risques numériques et d'en assurer le suivi régulier par les instances de gouvernance du GST, afin

d'éclairer la décision stratégique et d'orienter les actions correctives.

SOP n°3 : Gestion des accès et traçabilité des utilisateurs

La gestion des accès aux systèmes numériques du GST constitue un élément essentiel de la sécurité des systèmes d'information et de la protection des données de santé. Cette SOP encadre l'attribution, la modification et la suppression des droits d'accès aux applications, plateformes de données et outils d'intelligence artificielle, en fonction des missions et des responsabilités des utilisateurs. Elle repose sur une validation institutionnelle préalable des habilitations, une définition claire des rôles et des niveaux d'accès, ainsi que sur une traçabilité systématique des actions sensibles. La journalisation automatisée des accès et des opérations critiques permet de renforcer la responsabilité individuelle et collective, de prévenir les usages non autorisés et de soutenir les mécanismes de contrôle, d'audit et de gestion des incidents à l'échelle du GST[79].

SOP n°4 : Formation continue et sensibilisation du personnel

La procédure opérationnelle standard de formation continue et de sensibilisation du personnel a pour objectif d'assurer le développement continu des compétences des professionnels intervenant dans le traitement des données de santé, afin de garantir une gouvernance conforme, sécurisée et efficiente. Elle concerne tous les acteurs des Groupements Sanitaires Territoriaux, à savoir les professionnels de santé, le personnel administratif, les responsables des systèmes d'information et les chercheurs. Cette démarche s'appuie sur des principes fondateurs que sont l'actualisation régulière des connaissances, l'adaptation des contenus aux responsabilités des utilisateurs et la promotion d'une culture institutionnelle de la donnée fondée sur la responsabilité, la transparence et la sécurité.

Les programmes de formation doivent aborder des sujets clés, notamment la gouvernance des données de santé, la protection des données personnelles conformément à la réglementation en vigueur, la cybersécurité, la qualité et la traçabilité des données, ainsi que l'utilisation des systèmes d'information hospitaliers et les questions éthiques liées à l'exploitation des données, y compris dans le cadre des technologies d'intelligence artificielle. La mise en œuvre opérationnelle s'appuie sur l'élaboration d'un plan annuel de formation validé par la direction du GST, l'organisation de sessions régulières en présentiel ou à distance, l'intégration de modules obligatoires pour les étudiants et la mise en place de formations spécialisées pour les fonctions critiques, notamment en matière de protection des données et de gestion des systèmes d'information. Cette dynamique doit être renforcée par des partenariats avec des institutions académiques et des organismes spécialisés.

En plus des dispositifs formels, des actions continues de sensibilisation doivent être menées par la diffusion de supports pédagogiques, l'organisation d'ateliers pratiques et de simulations, et la mise en place de campagnes internes pour renforcer les bonnes pratiques numériques et la vigilance face aux risques. Ce dispositif est efficace grâce à un système d'évaluation organisé, comprenant des tests pour valider les acquis, le suivi des indicateurs de participation et des audits réguliers des pratiques. Les responsabilités sont clairement définies entre la direction des GST qui assure l'orientation stratégique et les ressources, le Délégué à la Protection des Données qui veille à la conformité, les responsables de formation, chargés de

la mise en œuvre, ainsi que les encadrants et le personnel, tenus de participer activement et d'appliquer les bonnes pratiques. Ce dispositif contribue in fine à renforcer les compétences, améliorer la qualité et la sécurité des données, réduire les risques opérationnels et instaurer une culture durable de gouvernance des données de santé.

SOP n°5 : Audit interne et amélioration continue

L'audit interne constitue un levier structurant de pilotage et d'amélioration continue des dispositifs numériques du GST. Il s'appuie sur une planification annuelle des audits, élaborée en début d'année, qui couvre l'ensemble des systèmes et processus numériques et priorise les interventions en fonction des risques identifiés dans la SOP n°2. Cette planification s'inscrit dans une approche méthodologique conforme aux lignes directrices de la norme ISO 19011 relatives à l'audit des systèmes de management, garantissant une démarche structurée, indépendante et fondée sur les risques. Chaque audit est ainsi défini avec des objectifs spécifiques, incluant la conformité réglementaire, la sécurité des données et la performance des outils numériques[80].

La réalisation des audits est assurée par des équipes internes formées à la gouvernance numérique, aux bonnes pratiques de cybersécurité et à la protection des données personnelles (loi 09-08). Les audits utilisent des checklists standardisées et portent sur les processus numériques, les usages de l'intelligence artificielle, les systèmes d'information et l'efficacité opérationnelle.

Les résultats des audits donnent lieu à des rapports formalisés qui présentent les constats, les écarts et les recommandations. Ces rapports sont diffusés aux responsables concernés, incluant le GST, la DSI et le DPO. Les recommandations sont traduites en plans d'actions ciblés, priorisés selon leur impact sur la sécurité, la conformité et la performance.

Le suivi des plans d'action est assuré via un tableau de bord permettant de vérifier la mise en œuvre effective des mesures correctives et préventives dans les délais fixés. L'efficacité de ces actions est régulièrement réévaluée et les SOP sont ajustées en fonction des résultats observés. Enfin, la SOP favorise la capitalisation et l'amélioration continue. Les retours d'expérience et les bonnes pratiques sont intégrés dans la mise à jour des SOP et partagés au niveau du GST pour harmoniser les processus numériques. Des audits périodiques permettent de mesurer la durabilité des actions et d'identifier de nouvelles opportunités d'amélioration, consolidant ainsi un modèle de gouvernance numérique hospitalière fondé sur la performance, la transparence et la durabilité[81].

3. Délégué à la Protection des Données (DPO)

Dans le contexte de l'intégration de l'intelligence artificielle et de l'amélioration de la gouvernance des données cliniques au sein des CHU, le rôle de Délégué à la Protection des Données (DPO) se positionne comme une composante essentielle garantissant la confiance et la transparence dans la transformation numérique du secteur de la santé.

Ce rôle ne se limite plus à la conformité réglementaire : Il représente la responsabilité éthique et institutionnelle d'assurer que l'utilisation de l'intelligence artificielle et des données médicales se conforme aux principes de sécurité, d'équité et de respect des droits des patients.

A. Désignation et positionnement institutionnel :

Le cadre juridique marocain actuel, notamment la loi n° 09-08, ne consacre pas explicitement la fonction de Délégué à la Protection des Données (DPO), bien qu'il impose l'identification d'un point de contact permettant l'exercice effectif des droits des personnes concernées[82].

Dans ce contexte, la mise en place d'un DPO au sein des établissements hospitaliers publics relève d'une recommandation de gouvernance, destinée à structurer et professionnaliser la gestion de la protection des données de santé[83]. Il est recommandé que le GST désigne un référent principal en matière de protection des données, afin de préserver son indépendance fonctionnelle, avec des relais organisationnels au niveau des pôles hospitaliers ou des Groupements Sanitaires Territoriaux (GST)[84].
Cette fonction recommandée s'inscrirait dans une logique de coordination avec les directions et instances concernées, notamment les systèmes d'information, l'éthique, l'information médicale et la qualité–gestion des risques[85].

Afin d'assurer une harmonisation nationale de cette fonction non encore consacrée par le droit positif, l'élaboration d'une Charte nationale des DPO hospitaliers, sous l'égide de la CNDP et des instances nationales compétentes, est recommandée. Cette charte aurait vocation à préciser les missions, les garanties d'indépendance et les modalités d'implication de ces référents dans la gouvernance stratégique des données et de l'intelligence artificielle en santé[86].

B. Missions et responsabilités :

Les Délégués à la Protection des Données (DPO) ont pour rôle de s'assurer de la conformité juridique des traitements de données conformément aux normes internationales (ISO 27701)[87], de superviser les projets d'intelligence artificielle, d'évaluer les risques éthiques et sécuritaires, ainsi que de coordonner avec les autorités compétentes.

Ils garantissent la traçabilité des algorithmes, veillent à ce que le consentement des patients soit respecté, et s'assurent que chaque système d'intelligence artificielle est piloté par un professionnel de santé expérimenté. Selon le RGPD (Règlement général sur la protection des données), le DPO a également pour mission d'informer et de conseiller le GST et le personnel sur leurs obligations en matière de protection des données, de sensibiliser aux bonnes pratiques et d'accompagner la conformité des traitements [88].

Dans le but de créer une cohérence à l'échelle nationale, il serait judicieux de mettre en place un Réseau national des DPO en santé. Ce réseau favoriserait la mutualisation des outils de conformité, faciliterait l'échange d'expériences entre les GST, et contribuerait à l'harmonisation des protocoles de gouvernance liés aux données et à l'intelligence artificielle [89].

De plus, une évaluation annuelle indépendante des DPO et de leurs méthodes renforcerait la transparence et permettrait d'identifier les besoins en développement des compétences.

C. Capacité institutionnelle et formation

Chaque GST pourrait s'appuyer sur une cellule fonctionnelle de coordination "Données et IA", à périmètre restreint, articulée autour :

- D'un référent principal en protection des données : DPO[90].
- D'un référent technique issu de la Direction des Systèmes d'Information, incluant les enjeux de sécurité et de cybersécurité[91].
- D'un appui juridique interne, assuré par la direction juridique existante du GST[92].
- D'un relais fonctionnel du DIM, en tant que division relevant du ministère de tutelle, sans remise en cause de son statut institutionnel[93].

Cette cellule aurait pour rôle de coordonner l'expertise technique, juridique et organisationnelle nécessaire à la mise en œuvre des projets numériques et d'IA, en veillant à la conformité réglementaire, à la qualité des données et à l'alignement éthique des usages[94].

S'agissant du renforcement des compétences, le MSPS en coordination avec les ministères concernés (Enseignement supérieur, Transition numérique) et les universités publiques, développe un dispositif national de formation continue en gouvernance des données de santé, cybersécurité et usages responsables de l'IA, à destination des cadres hospitaliers[95].

Enfin, le renforcement de la sécurité numérique hospitalière devrait s'inscrire dans les mécanismes de financement public existants ou futurs, dédiés à la transformation numérique du système de santé, sans création systématique de fonds spécifiques au niveau des établissements. Cette approche graduée permettrait de consolider durablement les capacités institutionnelles, tout en maîtrisant les coûts et en assurant la soutenabilité organisationnelle du modèle proposé[96].

D. Rapports de supervision vers le NH-DGC

Afin d'assurer une vision consolidée et stratégique de la gouvernance des données et des usages de l'intelligence artificielle au sein des GST , il est recommandé de mettre en place un mécanisme harmonisé de remontée d'information vers une instance nationale compétente en matière de gouvernance des données de santé, à définir ou à désigner dans le cadre des réformes en cours, à titre de fonction de pilotage et de coordination, sans préjuger de sa dénomination, de son statut juridique ni de son rattachement institutionnel[97].

Dans ce cadre, chaque CHU transmettrait, à un rythme semestriel, un rapport synthétique validé par le GST, portant sur :

- Conformité légale et sécurité : respect des normes, incidents signalés, mesures correctives mises en place et résultats des audits internes et externes.

- Qualité et performance des données : taux de complétude du *Minimum Clinical Data Set (MCDS),* des bases de données, interopérabilité et traçabilité des informations.

- Supervision des systèmes d'IA : description des algorithmes utilisés, validation clinique, évaluation éthique, et contrôle humain des décisions automatisées.

- Recommandations stratégiques : besoins en formation, ressources humaines, régulations et infrastructures identifiés[98].

Ces rapports doivent être accompagnés d'un tableau de bord national standardisé, permettant des comparaisons entre les régions et le suivi de la conformité. En cas d'incident majeur, le DPO doit informer la CNDP dans un délai maximal de 72 heures, conformément aux normes internationales (ISO 29134)[99].
En outre, la publication d'un rapport annuel sur la confiance numérique dans les hôpitaux, qui serait accessible au public, améliorerait la transparence et renforcerait la confiance des citoyens dans l'utilisation des technologies d'IA dans le domaine de la santé[100].

E. Gouvernance et amélioration continue

Chaque année, le ministère de la Santé et de la Protection sociale réalise une revue nationale de conformité, visant à uniformiser les pratiques, identifier les besoins en formation et évaluer l'impact des politiques publiques sur la gouvernance des données. Les résultats de cette évaluation donnent lieu à la publication d'un Rapport public sur la gouvernance et l'éthique de l'IA dans les hôpitaux, consolidant les informations issues des rapports des DPO[101].

Pour renforcer la cohérence stratégique, il est recommandé de créer un Conseil national d'éthique et de supervision de l'IA en santé, regroupant la CNDP, le ministère de la Santé et les universités. Ce conseil aurait pour mission de réglementer l'usage de l'IA, d'identifier et d'analyser les risques éthiques, et de formuler des recommandations publiques sur la transparence et la responsabilité des institutions[102].
Par ailleurs, la mise en place d'un Indice national de maturité numérique hospitalière (INMH) permettrait d'évaluer annuellement la conformité, la sécurité et l'éthique des établissements, tout en stimulant une dynamique de concurrence positive entre eux [103].
Enfin, il est essentiel de promouvoir une culture de responsabilité numérique, où chaque établissement rend publics ses engagements et ses pratiques. En combinant supervision, formation et implication citoyenne, cette approche garantit une transformation numérique du système de santé marocain éthique, inclusive et durable.

VIII. Huitième recommandation : Création et gouvernance des Entrepôts de Données de Santé (EDS) au niveau des GST

1. Contexte et levier des réformes sanitaires

La mise en place du Dossier Médical Partagé (DMP) et sa généralisation, conformément à la loi-cadre n° 06-22 relative au système de santé, s'inscrivent dans une stratégie nationale de digitalisation du système de santé. Cette initiative est soutenue par le Ministère de la Transition Numérique et de la Réforme de l'Administration, afin de répondre aux besoins croissants de la population et d'améliorer l'efficacité et la qualité des services de santé [104] [105].

La réforme prévoit la création d'une interface unifiée, permettant l'interopérabilité des solutions de DMP et de feuilles de soins électroniques au niveau national. Cette interface assure la connexion harmonisée avec les systèmes d'information des établissements de santé publics et privés, facilitant l'accès, le partage et l'utilisation sécurisée des données de santé [106] .

Cette démarche, cofinancée par la Banque mondiale dans le cadre du Programme de réforme du système de santé au Maroc (P179014), s'inscrit dans le Pilier 1 : Renforcement des capacités organisationnelles et institutionnelles pour la gouvernance du système de santé (ILD3), avec pour objectif l'amélioration du contenu, de la qualité, de l'accessibilité et de l'utilisation des données de santé. Le financement prévu pour cet indicateur est de 37,5 millions USD [107].

La création et la gouvernance des Entrepôts de Données de Santé (EDS) au niveau des Groupements de Santé Territoriaux (GST) constitue un levier stratégique pour renforcer la planification, le pilotage et la prise de décision fondée sur des données fiables et centralisées. Cette approche contribue à l'optimisation de la qualité des soins, à la coordination des acteurs et à la mise en œuvre efficace des politiques de santé publique.

2. Rôle et utilité stratégique des EDS

Les Entrepôts de Données de Santé Hospitaliers (EDSH) constituent une infrastructure stratégique essentielle pour les politiques publiques de santé, la recherche et l'innovation, ainsi que la surveillance épidémiologique[108]. Leur développement nécessite une attention particulière aux instruments réglementaires, aux capacités et expertises des ressources humaines, ainsi qu'à la mobilisation et à l'expertise technologique.

Les EDSH permettent le recueil et l'analyse d'un volume important de données (*Big Data*), intégrant des informations cliniques, socio-démographiques et médicales du patient. Ces données peuvent être utilisées pour la recherche et le développement scientifique, le pilotage et l'évaluation des activités de santé, ainsi que pour la gestion, le contrôle et l'administration des établissements [109].

Plusieurs pays ont déjà développé une expertise solide dans ce domaine, notamment la France, où la mise en œuvre des EDS est encadrée par la Commission Nationale de l'Informatique et des Libertés (CNIL) et soumise à son autorisation. Entre 2016 et 2025, 102 acteurs ont mis en œuvre un ou plusieurs EDS, représentant 125 entrepôts au total : 45 acteurs publics, 32 acteurs privés à but non lucratif et 25 acteurs privés à but lucratif [110].

Au regard du chantier structurant en cours dans le système de santé marocain, il est recommandé de mobiliser les acteurs publics et privés afin de promouvoir la création d'EDSH au Maroc et d'adopter des pratiques adaptées à l'organisation et à la gouvernance de ces infrastructures. Ces actions permettront de renforcer l'efficacité du système de santé, d'améliorer la qualité des soins et de stimuler la recherche scientifique nationale.

3. État des lieux au Maroc

Le Maroc dispose d'un portail *Open Data* (data.gov.ma)[111], qui inclut un groupe dédié à la santé, constituant une démarche positive vers la transparence et l'ouverture des données publiques. Cependant, les jeux de données disponibles restent limités en nombre, en nature et en actualité, étant principalement de nature administrative plutôt que clinique.

À ce jour, aucune source officielle de données individuelles de santé structurées n'est accessible publiquement, ce qui freine le développement de projets d'Entrepôts de Données de Santé Hospitaliers (EDSH) ou d'analyses épidémiologiques avancées basées sur des données locales.

Le portail data.gov.ma – Santé peut être considéré comme un indicateur institutionnel de l'état de l'ouverture des données de santé au Maroc, mais il ne constitue pas une base empirique suffisante pour une recherche scientifique fondée sur l'exploitation de données cliniques ou hospitalières.

4. Recommandations d'actions stratégiques

1. Introduction

Les entrepôts de données de santé (EDS) correspondent à des dispositifs permettant la mise en commun de données issues d'un ou de plusieurs systèmes d'information médicaux, organisées selon un format homogène afin d'en permettre la réutilisation à des fins de pilotage, de recherche ou de prise en charge des patients.
Si les registres spécialisés et les enquêtes auprès des patients apportent des informations essentielles pour répondre à des questions de recherche ciblées, ils nécessitent des efforts spécifiques de collecte. À l'inverse, les données médico-administratives ainsi que les dossiers patients informatisés (DPI) sont recueillis de manière routinière. Ces sources présentent l'avantage de couvrir des populations larges et diversifiées, sur des périodes de suivi prolongées, constituant ainsi un socle particulièrement riche pour les analyses en santé.

2. Role et utilité stratégique

La finalité principale d'un EDS est de faciliter l'accès aux données de santé afin de soutenir des travaux de recherche et des études visant l'amélioration du système de santé et de la qualité des soins délivrés aux patients. Le cadre d'exploitation des données issues des EDS a pour objectif de simplifier leur utilisation, d'en optimiser la gestion et d'en renforcer la valeur ajoutée, au bénéfice de la recherche médicale, de l'évaluation des pratiques et de l'aide à la décision.

Intérêt croissant des agences sanitaires pour les données de vie réelle

Au-delà des problématiques liées à l'évaluation des produits de santé, les données de vie réelle constituent aujourd'hui un levier majeur pour l'analyse de la qualité, de la sécurité et de la pertinence des soins. Elles permettent également la conduite d'études épidémiologiques observationnelles, la surveillance sanitaire, ainsi que le pilotage des politiques et des organisations de soins aux niveaux local et national.

3. Actions de mobilisation institutionnelle

En France, le Ministère de la Santé et de la Prévention a lancé en juillet 2022 un appel à projets doté de 50 millions d'euros, visant à structurer et renforcer un réseau d'entrepôts de données de santé hospitaliers coordonnés avec la Plateforme des Données de Santé (HDH) à l'horizon 2025 [112]. Ces appels à projets publics assurent la sécurisation, l'interopérabilité et la conformité réglementaire des EDSH, en s'appuyant sur des standards techniques tels que OMOP et FHIR.

Au Royaume-Uni, l'accès aux données repose sur des plateformes centralisées comme NHS Digital et le UK Biobank, combinant sécurité, consentement individuel (opt-out) et facilitation de la recherche (NHS England, 2023 ; UK Biobank, 2024). Ces modèles illustrent deux approches complémentaires de gouvernance des données de santé et fournissent des repères pour l'élaboration d'une politique adaptée au Maroc.

Pour le Maroc, il est recommandé d'orienter la politique publique autour des actions suivantes :

Rec.1 – Désignation de l'autorité nationale spécialisé

❑ Action stratégique recommandée :

Désigner la CNDP comme autorité nationale compétente pour délivrer les autorisations relatives à la mise en place et à l'exploitation des EDS au sein des établissements hospitaliers.

❑ Missions assurées :

- Élaborer ou adapter les textes et directives encadrant la collecte, le stockage, le partage et l'exploitation

des données de santé;

- Assurer le respect de la loi nationale sur les données personnelles, notamment en matière de consentement, confidentialité et pseudoanonymisation , et traçabilité des traitements ;
- Accompagner les ministères et parties prenantes dans le déploiement des EDSH;
- L'émission de référentiels permet aux organismes souhaitant mettre en œuvre un entrepôt de données de santé de s'assurer de la conformité de leur projet au cadre législatif et réglementaire en vigueur. Elle s'inscrit pleinement dans la mission permanente d'information et de sensibilisation de la CNDP, telle que prévue par la loi n° 09-08, promulguée par le Dahir n° 1-09-15 du 22 Rabii I 1430, notamment en son article 29.

❑ Objectif stratégique :

Garantir une mise en place encadrée et sécurisée des EDS, conciliant innovation en santé, protection des droits des citoyens et cadre clair pour l'utilisation des données à des fins de santé publique et de recherche.

Rec.2 – Lancer des appels à projets ciblés

❑ Actions recommandées :

Financer la structuration, la mise en conformité et la montée en capacité des EDSH via des appels à projets pilotés par le MSPS.

Ces appels doivent s'appuyer sur la mutualisation des budgets ministériels, notamment entre le MSPS et le Ministère de l'Énseignement Supérieur Recherche Scientifique et Innovation, afin de garantir efficacité, optimisation des ressources publiques et équité territoriale.

Rec.3 – Création d'un Comité National des Données de Santé

La création du comité est recommandée pour plusieurs finalité relatives à la valorisation et l'exploitation éthique des données de santé nationale, et orienter leur gouvernance vers des fins d'intérêt public.

❑ Benchmark Français : le Comité stratégique des données de santé.

Créé par arrêté ministériel en 2021[113] et placé sous la présidence du ministre de la Santé, ce comité accompagne le développement du Système national des données de santé (SNDS). Sa mission est de fédérer les acteurs publics et privés pour construire un patrimoine national de données de santé interconnectées, accessibles et de qualité, au service de la recherche, de la santé publique et de l'innovation. Il formule des recommandations concrètes pour améliorer la collecte, le partage et l'utilisation des données

à des fins d'intérêt public, notamment la création des EDS.

Les axes de travail de ce comité français constituent un fils conducteur pour esquisser un tissu institutionnel au Maroc visant une ambition similaire : construire un patrimoine national de données structuré et interconnecté, au service de l'intérêt général. Nous reconnaissons toutefois l'asymétrie institutionnelle et législative, entre le modèle français et le contexte marocain, qui en limitent le transfert direct et nécessitent une immersion et réflexion plus nuancé.

- Vision de la politique publique :

Dans le contexte marocain de décentralisation régionale, les données produites par les 11 régions convergent progressivement vers un Data Warehouse national. Sans gouvernance centrale, ces données risquent stagnation, fragmentation ou sous-exploitation. Compte tenu des défis liés aux capacités institutionnelles, aux ressources disponibles et au renforcement des missions des instances existantes, il est nécessaire de cibler les acteurs fondamentaux chargés de créer, piloter et structurer les Entrepôts de Données de Santé (EDS) à l'échelle nationale.

Un Comité National des Données de Santé (CNDS) constitue ainsi une nécessité institutionnelle et stratégique, garantissant le pilotage, la valorisation et la structuration du patrimoine national de données de santé.

- Actions Stratégiques recommandées :

Le CNDS agira en coordination avec la CNDP, les Directions Régionales de la Santé (DRS) et le MSPS, afin de propulser une phase nationale de structuration et de déploiement des EDSH au niveau des GST, en ciblant prioritairement les hôpitaux publics.

Ensuite, le Comité assurera la mise à l'échelle de ces structures, en fédérant les acteurs publics et privés et en répondant aux besoins des porteurs de projets, afin de construire un patrimoine national de données de santé interconnecté, au service de la recherche scientifique, de la santé publique et de l'innovation.

- Missions principales :

1. Orchestrer le développement et la cartographie stratégique des bases de données nationales et des EDSH, en garantissant équité territoriale dans leur déploiement et leur utilisation.
2. Régir et instituer les modalités d'accès aux données, afin de renforcer transparence, lisibilité et équité, tout en réduisant les barrières d'entrée pour les personnes physiques ou morales civiles.
3. Définir et promouvoir les standards de qualité et d'interopérabilité, en assurant leur compatibilité avec les normes nationales, pour favoriser la mutualisation, le partage, l'interconnectivité et l'exploitation durable des données à des fins de recherche et de santé publique.

Rec.4 – Favoriser la mutualisation et le partage inter-établissements

- Acteur concerné : Les Groupements Sanitaire Territoriaux (GST), CNDS.

Le comité mettra en œuvre des mécanismes d'incitation visant à initier et à promouvoir la conclusion d'accords multicentriques, ainsi qu'à instaurer une dynamique structurée de partage et d'interopérabilité des données entre les Groupements Sanitaires Territoriaux (GST) et les différents établissements de santé, publics et privés.

Rec.5 – Construire une expertise technique interne autour des données

- Acteur concerné : Les Groupements Sanitaire Territoriaux, MSPS

Former et investir dans des équipes internes capables de comprendre, documenter et faire évoluer les flux de données entre SI sources et EDSH.

Mutualiser ces compétences à l'échelle territoriale via la Division de l'Informatique et Méthodes (DIM).

Mobiliser l'expertise médicale, académique et des médecins spécialistes en Informatique Médicale sur les projets de structuration des EDSH.

Rec.6 – Instruments de financements et mise en capacité

- Acteurs concernés : GST, CNDS

- Actions recommandées :

Pour déployer les Entrepôts de Données de Santé Hospitaliers (EDSH) au sein des Groupements Sanitaires Territoriaux (GST), il est recommandé de combiner financement autonome, partenariats publics-privés (PPP) et gouvernance encadrée :

1. Financement autonome et interne

Mobiliser les budgets propres des GST dédiés à l'informatique et aux infrastructures hospitalières.

Réaffecter des ressources existantes pour soutenir les projets pilotes et la montée en capacité.

2. Partenariats Public-Privé (PPP)

Collaborer avec des prestataires privés pour expertise technique, intégration et maintenance des EDSH.

Encadrer ces contrats afin de protéger la souveraineté numérique, limiter la dépendance et garantir que les

prestations servent l'intérêt public.

Inclure systématiquement la documentation et mise à jour des schémas de données, ainsi que des clauses contractuelles transparentes et claires sur la propriété et les droits d'usage des données.

4. Etapes de structuration des EDSH

Afin d'assurer une infrastructure sécurise des données, il est proposé de suivre une data pipeline basée sur un processus ETL (*Extract, Transform, Load*) standardisé.

L'infrastructure des Entrepôts de Donnée de Santé (EDS) sera basée sur ce pipeline ETL pour ingérer les données des différents SIH (Systèmes d'Information Hospitalier) via des API FHIR. Les procédures du ETL forme le principal mécanisme qui veille à ce que les données des hôpitaux soient disponibles, standardisées, et sécurisées pour tout utilité, qu'elle soit pour analytique, coordination ou prise de décision.

❑ Ce processus fonctionne en trois étapes :

Extraction : l'objectif de cette étape est d'extraire les données depuis différents systèmes d'information hospitaliers. Les sources typiques incluent les dossiers de santé électronique, les systèmes d'information patients, les systèmes de laboratoires, les pharmacies et les bases de données inventaire. Pour ce faire, une connexion sécurisée en utilisant des API FHIR, une extraction des outils pour être sûr d'une traçabilité et une transparence.

Transformation : cette étape nettoie et structure les données extraient pour qu'elles soient cohérentes. Naturellement les transformations veilleront à supprimer tous les doublons, assurer une normalisation par convertir toute donnée en standard médical, la pseudonymisation / anonymisation et la validation pour vérifier la qualité clinique et la consistance logique ;

Chargement : les données transformées sont chargées dans les EDS. Plusieurs types de chargement sont reconnues :

1. Chargement initial : qui a un historique complet de la population de donner.
2. Chargement incrémental : qui est chargé de faire des mises à jour régulières.
3. Chargements en temps réel : pour les données qui sont classifies temps-sensibles.

Ainsi, pour un respect est une conformité et obligations légales chaque chargement sera traçable, journalisé et audité.

5. Principes de gouvernance technique

Introduction

Les données intégrées dans l'EDSH proviennent d'extractions automatisées des systèmes d'information hospitaliers (SIH). Les difficultés de réutilisation sont donc liées à la complexité, l'hétérogénéité et la documentation (ou son absence) des SI sources.

La gouvernance technique vise à garantir l'exploitation cohérente, sécurisée et interopérable des données cliniques, en s'appuyant sur des standards nationaux et internationaux et une organisation claire des responsabilités.

Recommandations de bonnes pratiques

REC.1 – GÉRER LA COMPLEXITÉ DES SYSTÈMES SOURCES

Les transformations de données depuis les SI sources vers les jeux de données d'étude sont peu documentées publiquement. La possibilité de mobiliser les données collectées en routine dépend de leur degré de concentration, allant de la centralisation dans un SI unique et homogène à l'éclatement dans une multitude de SI aux formats hétérogènes. La structure des SI reflète celle de la gouvernance. La facilité à travailler sur ces données dépend fortement de l'organisation des acteurs du soin.

❑ Actions recommandées :

Supporter la performance et la robustesse des bases de données régionales et décentralisées, au niveau de chaque GST. Assurer le support régional des traitements de données depuis plusieurs SI sources vers l'extraction des jeux de données des EDS.
Mise en place de plateformes d'échange et de coordination organisées entre les entités centrales et régionales, sous l'égide du MSPS, et la gouvernance technique spécialisée de la Direction de l'Informatique et des Méthodes (DIM).

Rec.2 – Reconnaître le pluralisme des modèles et promouvoir l'interopérabilité

L'adoption d'un modèle standard permet d'améliorer la production et le partage de connaissances entre organisations dont les personnels sont fortement mobiles. Les hôpitaux et instituts de recherche utilisent différents modèles internationaux (I2B2, OHDSI-OMOP, Sentinel, PCORnet).

❑ Actions recommandées :

Adoption et généralisation du modèle OMOP comme standard initial.

Développer des connecteurs et pipelines de transformation pour assurer la compatibilité entre différents modèles (ex. FHIR ↔ OMOP).

Favoriser le mapping standardisé entre modèles afin de participer aux études multicentres internationales

sans dépendre d'un modèle unique.

Maintenir une bibliothèque partagée de mappings et transformations réutilisables.

❑ Acteurs **:** CNDS, équipes DIM, data architects.

Rec.3 – Adopter un socle national de données cliniques par les hôpitaux

En France, un groupe de travail piloté par le *Comité stratégique des données de santé* a défini un socle commun de 51 variables (données démographiques, cliniques, médicamenteuses, etc.) destiné à harmoniser la collecte dans les entrepôts de données hospitaliers.

❑ Actions recommandées :

Généraliser l'adoption d'un Socle National de Données Cliniques (*Minimum Clinical Data Set*) conforme et scalable, servant d'architecture commune pour les catégories de données alimentant les EDSH. Ce socle vise à améliorer l'interopérabilité et la qualité des données hospitalières réutilisées en recherche et pilotage.

Acteurs concernés : Comité National des données de santé (mandaté par arrêté et pouvoirs publics), et les équipes spécialisées de la DIM-MSPS.

Rec.4 – Combler le déficit sémantique

Prioriser la standardisation sémantique (nomenclatures, terminologies).

❑ Action recommandée :

Instituer un socle national de nomenclatures (CIM, CCAM, LOINC, SNOMED).

Rec.5 – Clarifier les normes et les standards adoptés par les hôpitaux

❑ Action recommandée :

- Développer les normes nationales pour l'accompagnement technique et réglementaire des projets de structuration des EDSH.
- Élaborer un référentiel national de la qualité des données EDSH, couvrant normes de qualité, maintenance et conformité aux standards.

Rec.6 – Investir dans la gouvernance des modèles

❑ Action recommandée :

- Créer des instances de gouvernance.
- Financer des data architects et data stewards.

6. Infrastructure et sécurité

1- Principes d'infrastructure

L'infrastructure technique du système repose sur un socle de serveurs (virtuelles ou physiques), qui hébergeront tous logiciels qui permettront au système de fonctionner proprement et en toute sécurité. Les exigences gouvernants l'architecture, l'hébergement, l'anonymisation et la traçabilité s'illustrent dans l'architecture conçue.

2-Architecture fondamental :

Les entrepôts des données de santé (EDS) déployé au niveau du GST promet une interopérabilité technique entre toutes les institutions, hôpitaux, cliniques, laboratoires, et parfois les autorités de santé régionale qui auront tous des systèmes différents certains standards de support seront nécessaires, des API pour standardiser les données venantes, et un *Index Patient Master* pour identification et unification sur tous les sites.

3- Conformité d'hébergement

L'hébergement de l'EDS et des composants critiques doit obligatoirement être certifié Hébergement des Données de Santé (HDS) ou répondre à un référentiel de sécurité équivalent, garantissant ainsi la souveraineté nationale et la protection physique des données sensibles.

4-Couche de sécurité technique

4.1- Couche d'authentification et d'autorisation :

Cette couche gère la vérification d'identité et les permissions d'accès.

i. Cadre technique : OAuth 2.0 avec OpenID Connect (OIDC)
ii. Jetons d'accès (JWT) : Jetons à durée de vie courte (par exemple, 1 heure) contenant les rôles et permissions de l'utilisateur. Ce sont des paquets JSON signés cryptographiquement et validés rapidement par la passerelle API.
iii. Jetons d'actualisation : Jetons opaques à longue durée de vie, stockés de manière sécurisée sur le client. Utilisés pour obtenir silencieusement de nouveaux jetons d'accès sans intervention de l'utilisateur, ils offrent un équilibre entre sécurité et expérience utilisateur. Ils peuvent être révoqués instantanément via une base de données centrale.

iv. Point d'application : La passerelle API agit comme un point d'application des politiques (PEP) centralisé, validant chaque requête entrante avant qu'elle n'atteigne le SIH ou le SIA.

4.2- couche de sécurité transport :

Cette couche protège les données lors de leur transfert entre les systèmes.

i. Protocole : TLS 1.3
ii. Objectif : Chiffrer toutes les données en transit entre les clients, la passerelle API, les services d'IA et le SIH.
iii. Échange de clés : Utilisé par défaut des algorithmes modernes et performants comme la cryptographie à courbe elliptique (ECC) pour l'établissement de la connexion initiale.
iv. Chiffrement des données : Le chiffrement symétrique est effectué automatiquement au sein du protocole TLS une fois le canal sécurisé établi.

4.3- couche de sécurité opérationnelle :

Contrôles de surveillance, d'enregistrement et de protection du système.

i. Sécurité réseau : Pare-feu et segmentation du réseau pour créer des zones sécurisées (par exemple, isolation du réseau de données cliniques).
ii. Journalisation et surveillance des audits (SIEM) : Chaque événement d'authentification, émission et utilisation de jeton, ainsi que toute tentative d'accès aux données, est enregistré et surveillé en temps réel afin de détecter les anomalies.
iii. Limitation du débit et limitation de la bande passante : Mise en œuvre au niveau de la passerelle API pour prévenir les attaques par déni de service (DoS) et les abus d'API.

5- Journalisation :

5.1- Les exigences d'audit se manifestent :

i. Toutes les tentatives d'authentification (succès/échec)
ii. Émission, actualisation et révocation de jetons
iii. Chaque appel d'API
iv. Changements de rôle et modifications d'autorisations

5.2- Les mesures de conformité :

i. Pseudonymisation systématique des données patients dans les journaux
ii. Suppression automatique des jetons expirés

7. Mesures de valorisation et transparence des EDSH

Introduction

En vue de renforcer la confiance, faciliter l'accès pour la recherche et optimiser l'usage des informations

de santé publique.

Rec.1 – Guichet unique

Il est recommandé d'instaurer un guichet unique en tant que point d'entrée centralisé pour l'accès aux données issues des EDSH.

Ce dispositif permettra notamment :

Un traitement harmonisé des demandes d'accès aux données ;

Une évaluation systématique par un comité scientifique et éthique compétent ;

La mise en œuvre de procédures standardisées, claires et traçables, garantissant l'équité, la conformité réglementaire et la sécurité juridique des projets.

Le guichet assure traçabilité, équité et sécurité juridique, tout en simplifiant l'accès pour la recherche et l'innovation.

Rec.2 – Transparence des études

Il est recommandé de mettre en place une publication centralisée et accessible des projets, études et travaux s'appuyant sur les données des EDSH.

Cette mesure vise notamment à :

Assurer la visibilité des usages des données de santé ;

Harmoniser les références et métadonnées avec les portails nationaux, répertoires institutionnels et bases internationales ;

Garantir une mise à jour régulière des informations relatives aux études en cours et achevées.

Rec.3 –Clarification des catégories d'usage des données des EDSH

Définir explicitement les usages autorisés des données au sein de chaque EDSH, en distinguant au minimum :

1. Recherche scientifique et académique ;
2. Projets partenariaux avec des acteurs privés ou associatifs ;
3. Veille épidémiologique et santé publique. Action étatique ;

4. Développement et déploiement d'outils de traitement automatique massives.

Établir un cadre d'autorisation spécifique pour chaque catégorie, avec des procédures adaptées aux risques et enjeux éthiques et réglementaires.

Documenter et publier les catégories et cas d'usage pour garantir la transparence auprès des patients, des chercheurs et des acteurs institutionnels.

Harmoniser les pratiques au niveau national via le Comité National des Données de Santé (CNDS), pour assurer cohérence, interopérabilité et mutualisation des données.

Pour la validation, valorisation et utilisation du système, les conditions d'accès sont différentes selon les profils. Ceci est une implémentation du principe *Least-Privileged* et *Purpose-Limitation* de la part de la CNDP, elle suggère que pas tous les profils nécessitent les mêmes données. Par conséquent l'accès est une fonction de rôle, de contexte et de raison. Différents types de profils existent au sein du système, qu'ils soient chercheurs, autorité de santé, partenaire commercial ou acteur au sein de l'hôpital. Chaque accès, à un but que ce soit la recherche, la maintenance du service, ou la surveillance de la santé publique. Les chercheurs ont accès à des données pseudonymisées, quant aux partenaires auront des données anonymisées. Tout en appliquant le consentement décrit dans le contrat entre le patient et le CHU.

Ses règles sont liées au design technique, ils forment le mécanisme du RBAC/ABAC Elle se rend configuré au sein de la passerelle API qui agit comme le point d'entrée des applications.

Lorsqu'une requête arrive depuis un utilisateur, la passerelle extrait le jeton JWT et vérifie les limites OAuth 2.0 qui pourrons définir le périmètre autorisé du FHIR ainsi que les attributs de l'utilisateur puis prendre une décision sur l'acceptation et la validation ou le refus d'accès de l'utilisateur.

Par exemple, un chercheur aura accès aux observations et aux conditions, mais pas aux données identifiantes des patients.

Un partenaire commercial aura accès aux appareils et un point à payer. Pour les métriques techniques. Toutes les données techniques ne sont ni anonymisées ni pseudonymisées.

Une autorité de santé ou réaction aux observations à grègues pour la surveillance épidémiologique, toute donné identificatoire des données sera anonymisée.

Le médecin aura accès aux données des patients sur les observations, les conditions et les requêtes des médicaments, pour une finalité de soin direct, et par conséquent, toutes les données seront identifiables. Chaque donnée accéder par quiconque, sera journalisé comme mécanisme de recevabilité et traçabilité.

8. Directives destiné à la CNDP

Introduction

Coordination entre CNDP, le Comité National des Données de Santé (CNGD), une entité d'où la création est recommandée (*voir section : 3. Action de mobilisation institutionnelle, Rec. 3)*, la Haute Autorité de Santé (HAS) et acteurs hospitaliers, notamment les GSTs.

Le Benchmark étudié est la France : La CNIL collabore avec Health Data Hub et HAS[114] .

Rec.1 – CNDP comme autorité compétente

La CNDP doit être formellement investie du rôle d'autorité de référence pour l'instruction et l'autorisation des EDSH, en cohérence avec ses attributions légales au titre de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. À ce titre, elle exercerait quatre fonctions essentielles :

En premier lieu, l'instruction et l'autorisation des EDSH, impliquant l'examen systématique de chaque demande de création ou d'extension d'un entrepôt, sur la base d'un dossier standardisé couvrant les finalités du traitement, les catégories de données collectées, les mesures de sécurité mises en œuvre et les modalités d'accès aux données.

En deuxième lieu, la coordination avec le Comité National de Gouvernance des Données (CNGD) et la Haute Autorité de Santé (HAS), afin d'assurer la cohérence entre les exigences de protection des données personnelles, les standards de qualité des données de santé, et les orientations stratégiques nationales en matière de santé numérique.

En troisième lieu, le contrôle du respect de la législation nationale par les établissements hospitaliers hébergeurs d'EDSH, notamment à travers des audits périodiques, des inspections sur site et l'examen des registres de traitements tenus par les Délégués à la Protection des Données (DPD).

En quatrième lieu, la surveillance du respect de l'obligation d'information des patients quant à la réutilisation secondaire de leurs données de santé — obligation dont la méconnaissance constitue un manquement grave aux droits fondamentaux des personnes concernées et expose les établissements à des sanctions administratives.

Rec.2 – Émettre les Référentiels nationaux de conformité

Il est recommandé d'élaborer et de publier des référentiels nationaux de conformité à destination des hébergeurs d'entrepôts de données de santé (EDS), afin de traduire les exigences de la législation nationale en prescriptions opérationnelles claires et en bonnes pratiques attendues. Ces référentiels devraient couvrir prioritairement les thématiques de la sécurité, de la pseudonymisation, de l'interopérabilité et de la traçabilité. Leur adoption effective devrait être conditionnée à l'octroi des financements publics, afin de garantir une mise en œuvre réelle et non symbolique. Ils devraient également servir de base à l'harmonisation des pratiques au sein des Groupements de Santé de Territoire (GST), en réduisant les

disparités entre établissements. Enfin, ils devraient intégrer des prescriptions spécifiques à la prévention des atteintes aux droits et libertés des personnes concernées, en déclinant les dispositions de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans le contexte propre aux données de santé.

ROYAUME DU MAROC

Feuille de Route Opérationnelle pour la Gouvernance Numérique Hospitalière

Plan de mise en œuvre national — Horizon 2026–2030

Contexte et principes directeurs

La présente feuille de route opérationnelle traduit la stratégie nationale de gouvernance numérique hospitalière en un programme d'action séquentiel, piloté et évaluable. Elle s'inscrit dans le cadre de la Loi-cadre n° 06-22 relative au Système National de Santé et de la Stratégie Digital Morocco 2030, et s'aligne sur les standards internationaux promus par l'OMS, l'OCDE et la Banque mondiale en matière de transformation numérique des systèmes de santé.

L'approche retenue repose sur quatre principes fondateurs :

- Progressivité et séquentialité : chaque phase conditionne la suivante, permettant de valider l'architecture technique et organisationnelle avant tout déploiement à grande échelle.
- Redevabilité et mesurabilité : chaque phase est assortie d'indicateurs de performance (KPIs) quantitatifs et qualitatifs, soumis à évaluation indépendante.
- Coordination institutionnelle : le MSPS, l'ADD, la CNDP, la DGSSI et l'ANRT exercent des rôles complémentaires et non substituables.
- Inclusion territoriale : les zones rurales et à faible connectivité font l'objet de mesures spécifiques dès la Phase 1.

Matrice de gouvernance institutionnelle

Le tableau ci-dessous présente la répartition des responsabilités entre les acteurs institutionnels pour l'ensemble du programme.

Institution	Rôle principal	Domaine d'intervention	Mécanisme de coordination	Fréquence de reporting
MSPS	Pilotage stratégique et cadre réglementaire	Gouvernance globale, protocoles nationaux	Comité de pilotage national (CPN)	Mensuelle
ADD	Architecture technique et interopérabilité	SIH, HL7 FHIR, MCDS, MPI	Comité technique interministériel	Bimensuelle
CNDP	Conformité juridique et éthique	Protection des données, RGPD, IA éthique	Audits trimestriels de conformité	Trimestrielle
DGSSI	Cybersécurité et résilience des systèmes	ISO 27001, gestion des incidents	Cellule de veille sécurité (CVS)	Continue + rapport mensuel
ANRT	Connectivité et performance réseau	Infrastructure télécom, zones rurales	Tableau de bord réseau national	Mensuelle
MESRSI	Formation et renforcement des capacités	Curricula, certification, littératie numérique	Comité pédagogique national	Semestrielle
HCP / Cour des Comptes	Suivi-évaluation et audit indépendant	KPIs nationaux, conformité budgétaire	Rapports annuels publics	Annuelle

Phase 1 — Validation du modèle de gouvernance numérique (Mois 1–18)

1.1 Objectif stratégique

Démontrer la viabilité technique, organisationnelle et juridique du cadre de gouvernance numérique hospitalière dans deux GST pilotes stratégiquement sélectionnés, et produire un référentiel de bonnes pratiques national, réplicable et documenté.

1.2 Sites pilotes retenus

#	Établissement	Rôle dans le pilote	Justification	Point de vigilance
1	**GST Tanger-Tétouan-Al Hoceima (Site pilote initial de lancement)**	Site de lancement initial du déploiement des GST ; validation du modèle opérationnel en conditions réelles	GST inauguré en 2023 avec infrastructure hospitalière moderne (CHU Mohammed VI) ; absence d'héritage technique contraignant ; représente le pôle Nord et offre un terrain idéal pour un déploiement natif des standards numériques	Absence d'historique numérique : accompagnement renforcé des équipes requis dès J+1 ; nécessité de constituer une base de données patients de référence dès les premiers mois
2	**GST Rabat-Salé-Kénitra (Site de support technique et de référence)**	Centre de support technique et de proximité ; appui méthodologique au site pilote de Tanger et hub de compétences pour la généralisation	GST de la capitale administrative ; CHU Ibn Sina stabilisation post-déménagement (2026) ; densité institutionnelle et proximité des ministères (MSPS, ADD, CNDP) facilitant la coordination ; capacité technique avantageuse pour accueillir le centre de support national	Transition physique du CHU Ibn Sina à intégrer dans le calendrier de déploiement ; risque de disponibilité des équipes IT durant la période de réorganisation interne

1.3 Plan d'action détaillé — Phase 1

Mois	Action	Acteur responsable	Livrable attendu	Critère de validation

1–2	Signature des conventions de partenariat entre MSPS et les 2 GST pilotes	MSPS / Direction CHU	2 conventions signées	Conventions juridiquement exécutoires, avec clauses de confidentialité CNDP
1–3	Audit de l'existant : cartographie des SIH, données, flux et infrastructures réseaux	ADD + DGSSI	Rapport d'audit technique par site	Rapport validé par le CPN ; gaps d'interopérabilité identifiés et priorisés
2–4	Désignation des Délégués à la Protection des Données (DPD) dans chaque CHU pilote	CNDP + Direction CHU	2 DPD opérationnels	DPD formés, accrédités par la CNDP et enregistrés dans le registre national
3–8	Déploiement des entrepôts de données hospitaliers normalisés (MCDS / MPI)	ADD + équipes techniques CHU	2 entrepôts opérationnels	Conformité HL7 FHIR vérifiée ; taux de couverture MCDS ≥ 80 % des dossiers actifs
4–10	Développement et déploiement de la couche d'interopérabilité unifiée entre SIH hétérogènes	ADD (maîtrise d'œuvre)	API d'interopérabilité nationale (v1.0)	Échanges réussis entre GST Tanger et GST Rabat-Salé-Kénitra ; latence < 500 ms
6–12	Mise en œuvre du programme de formation initial du personnel (gouvernance des données, cybersécurité, éthique IA)	MSPS + MESRSI + CHU pilotes	Programme de formation déployé, 500 agents formés	Taux de formation ≥ 70 % du personnel cible ; score de satisfaction ≥ 3,5/5
10–14	Évaluation intermédiaire indépendante et revue des	HCP / Cabinet externe mandaté par MSPS	Rapport d'évaluation à mi-parcours	Rapport publié, recommandations intégrées dans le plan de déploiement Phase 2

	indicateurs de performance			
14–18	Documentation du modèle opérationnel : référentiel de bonnes pratiques national	MSPS + ADD + CNDP	Référentiel national v1.0 publié	Référentiel validé par le CPN ; disponible en open access sur portail MSPS

1.4 Indicateurs clés de performance (KPIs) — Phase 1

Indicateur	Valeur de référence	Cible Phase 1	Source de vérification	Fréquence
% dossiers patients conformes au MCDS	0 %	**≥ 80 %**	Rapports ADD	Mensuelle
Disponibilité du système SIH (uptime)	Variable par site	**≥ 99,5 %**	Logs DGSSI	Continue
Temps de réponse moyen de l'API interopérabilité	Non mesuré	**< 500 ms**	Tests ADD	Hebdomadaire
Nombre d'incidents de sécurité critiques	Non mesuré	**0 incident critique non résolu sous 24h**	Rapports DGSSI	Continue
Taux de conformité CNDP des traitements	Non évalué	**100 % des traitements déclarés**	Audits CNDP	Trimestrielle
% personnel cible formé	0 %	**≥ 70 %**	Registres formation MSPS	Semestrielle
Taux d'adoption du SIH par les cliniciens	Variable	**≥ 65 %**	Enquête terrain	Trimestrielle

Nombre de DPD opérationnels et accrédités	0	**2 (1 par GST pilote)**	Registre CNDP	Unique / M4
Délai moyen d'échange inter-SIH	Non mesuré	**< 2 heures**	Logs ADD	Hebdomadaire

Phase 2 — Structuration de l'infrastructure nationale d'interopérabilité (Mois 19–36)

2.1 Objectif stratégique

Construire et déployer une architecture nationale intégrée permettant l'échange fluide, sécurisé, tracé et conforme des données de santé entre établissements hospitaliers, laboratoires, pharmacies et organismes de protection sociale (AMO, assurances privées), sur la base du modèle validé en Phase 1.

2.2 Plan d'action détaillé — Phase 2

Mois	Action	Acteur responsable	Livrable attendu	Critère de validation
19–21	Conception détaillée de la plateforme nationale d'interopérabilité (PNI) sur la base des retours Phase 1	ADD (maîtrise d'ouvrage) + prestataires certifiés	Architecture technique PNI v2.0 validée	Architecture approuvée par le CPN et conforme HL7 FHIR R4 / IHE
20–24	Déploiement de l'infrastructure télécom sécurisée pour les établissements en zones rurales et éloignées	ANRT + DGSSI	Plan de connectivité rurale opérationnel	100 % des établissements pilotes connectés avec débit ≥ 10 Mbps ; mode hors-ligne déployé
21–30	Intégration de la PNI avec les systèmes AMO (CNSS, CNOPS) et les assurances privées	MSPS + ADD + AMO	Protocoles d'échange AMO actifs	Échanges AMO opérationnels dans les 2 GST pilotes ; délai de remboursement réduit de 20 %

22–32	Déploiement du cadre de cybersécurité national conforme ISO 27001 dans tous les établissements connectés	DGSSI	Certification ISO 27001 des 2 GST pilotes	2 GST pilotes certifiés ou en cours de certification ISO 27001 à M32
25–34	Mise en service du Centre de support national (helpdesk L1/L2, catalogue national, veille réglementaire)	MSPS + ADD	Centre de support opérationnel	Taux de résolution des tickets L1 ≥ 80 % sous 4h ; SLA publié et auditable
30–36	Évaluation externe de Phase 2 et certification de l'infrastructure pour passage en Phase 3	HCP + Cour des Comptes + OMS	Rapport d'évaluation Phase 2 certifié	Infrastructure nationale déclarée apte au déploiement généralisé par l'évaluateur externe

2.3 KPIs — Phase 2

Indicateur	Valeur de référence	Cible Phase 2	Source de vérification	Fréquence
Nombre d'établissements connectés à la PNI	2 (pilotes)	**≥ 15**	Rapports ADD	Mensuelle
Débit minimum garanti — zones rurales	< 2 Mbps (certaines zones)	**≥ 10 Mbps**	Mesures ANRT	Trimestrielle
Disponibilité de la PNI (uptime)	N/A	**≥ 99,9 %**	Logs DGSSI	Continue
Délai moyen d'échange inter-établissements	Non mesuré	**< 30 minutes**	Logs ADD	Mensuelle

% établissements avec certification ISO 27001	0 %	**100 % des pilotes (M32)**	DGSSI	Unique / M32
Volume de transactions AMO traitées via PNI	0	**≥ 10 000 / mois (M30)**	Rapports AMO	Mensuelle
Taux de résolution tickets support L1 < 4h	N/A	**≥ 80 %**	Helpdesk national	Hebdomadaire
Nombre d'incidents de sécurité majeurs	Non mesuré	**0 non résolu sous 24h**	Rapports DGSSI	Continue

Phase 3 — Renforcement des capacités institutionnelles et humaines (Mois 25–42)

3.1 Objectif stratégique

Constituer un capital humain pérenne, compétent et certifié, capable d'opérer, de maintenir et de faire évoluer le système national de gouvernance numérique hospitalière. Cette phase se déploie en parallèle de la Phase 2 à partir du Mois 25, afin d'anticiper les besoins en compétences pour la généralisation (Phase 4).

3.2 Architecture du programme national de formation

Module	Contenu	Public cible	Modalité et durée
Module 1 Gouvernance des données de santé	MCDS, MPI, classification, droits d'accès, traçabilité	DIM, informaticiens médicaux, directeurs SI	Présentiel + e-learning — 40h
Module 2 Cybersécurité hospitalière	ISO 27001, gestion des incidents, DGSSI référentiel	RSSI, équipes IT, direction	Présentiel — 32h + certification
Module 3 Protection des données personnelles	Loi 09-08, RGPD comparé, droits des patients, DPD	DPD, juristes, responsables traitements	Présentiel — 24h + accréditation CNDP

Module 4 Éthique et gouvernance de l'IA en santé	Cadre OMS/OCDE, biais algorithmiques, consentement éclairé	Médecins, infirmiers, décideurs	E-learning — 16h
Module 5 Interopérabilité et standards (HL7 FHIR)	HL7 FHIR R4, IHE, SNOMED CT, LOINC, CIM-10	Développeurs SIH, informaticiens	Présentiel technique — 48h
Module 6 Littératie numérique de base	Utilisation SIH, sécurité des postes, gestion des mots de passe	Ensemble du personnel soignant et administratif	E-learning — 8h (obligatoire)

3.3 KPIs — Phase 3

Indicateur	Valeur de référence	Cible Phase 3	Source de vérification	Fréquence
Nombre d'agents formés (tous modules confondus)	0	**≥ 5 000 à M42**	Registres MSPS/MESRSI	Semestrielle
% personnel soignant ayant complété Module 6	0 %	**100 % à M42**	Plateforme e-learning	Trimestrielle
Nombre de DPD accrédités CNDP au niveau national	2 (pilotes)	**≥ 30**	Registre CNDP	Semestrielle
Nombre de RSSI certifiés ISO 27001 en milieu hospitalier	0	**≥ 15**	DGSSI	Annuelle
Score moyen de littératie numérique (enquête standardisée)	Non mesuré	**≥ 3,5 / 5**	Enquête MSPS/MESRSI	Annuelle
Nombre de CHU opérant comme centres de formation régionaux	0	**2 (les GST pilotes)**	MESRSI	Unique / M36
Taux de rétention du personnel formé (12 mois post-formation)	Non mesuré	**≥ 80 %**	DRH des établissements	Annuelle

Partenariats OMS/OCDE actifs pour benchmarking/certification	0	**≥ 2**	MSPS	Annuelle

Phase 4 — Généralisation nationale à l'ensemble des GST (Mois 37–72)

4.1 Objectif stratégique

Déployer le système national de gouvernance numérique hospitalière à l'ensemble des 12 régions sanitaires du Royaume selon un calendrier échelonné sur trois ans, en garantissant une appropriation locale effective, une couverture territoriale équitable et une évaluation annuelle indépendante.

4.2 Calendrier de généralisation — Critères de priorisation et conditions

Année	Périmètre de déploiement	Critères de priorisation	Conditions préalables	Résultat attendu mesurable
Année 1 (M37–M48)	GST à forte maturité numérique : Casablanca-Settat, Souss-Massa (+ GST pilotes Tanger et RSK)	Maturité SIH ≥ niveau 3 ; connectivité réseau garantie ; équipe IT en place	Package de déploiement standardisé validé ; centre de support national opérationnel	≥ 5 GST connectés à la PNI ; ≥ 70 % dossiers conformes MCDS ; 0 incident critique non résolu
Année 2 (M49–M60)	Majorité des GST : Fès-Meknès, Marrakech-Safi, Oriental, Béni Mellal-Khénifra, Rabat-Salé-Kénitra (élargissement), Tanger-Tétouan-Al Hoceima (élargissement)	Retours d'expérience Année 1 intégrés ; package de déploiement v2 disponible	ANRT a validé la connectivité de toutes les zones couvertes ; équipes formées en place	≥ 10 GST connectés ; taux d'adoption cliniciens ≥ 65 % ; ≥ 1 000 échanges inter-GST / mois
Année 3 (M61–M72)	GST restants avec accompagnement renforcé : Drâa-Tafilalet, Guelmim-Oued Noun, Laâyoune-Sakia El Hamra, Dakhla-Oued Ed-Dahab	Zones à faible maturité numérique ou connectivité limitée : mode hors-ligne préalablement testé et validé	Mode dégradé hors-ligne déployé et certifié DGSSI ; accompagnement organisationnel renforcé (ratio 1 expert pour 2 GST)	Couverture nationale à 100 % des 12 GST ; ≥ 80 % dossiers conformes MCDS à l'échelle nationale

4.3 Package de déploiement standardisé — Composantes

Chaque GST reçoit un package de déploiement préconfiguré, validé lors des phases précédentes et adaptable aux spécificités locales. Il comprend :

- Infrastructure technique : serveurs préconfigurés, connecteurs PNI certifiés, kit de mise en service
- Gouvernance locale : modèle de charte de gouvernance des données, procédures de gestion des incidents, registre des traitements CNDP
- Formation : accès à la plateforme e-learning nationale, module de formation des formateurs (ToT), référent numérique désigné
- Support : contrat de niveau de service (SLA) avec le centre de support national, accès au catalogue national
- Suivi-évaluation : tableau de bord KPIs précâblé, connecté au système de reporting national

4.4 KPIs — Phase 4 (Indicateurs nationaux consolidés)

Indicateur	Référence M0	Cible An 1	Cible An 2	Cible An 3	Source
Nombre de GST connectés à la PNI	3	≥ 5	≥ 10	**12 (100 %)**	ADD
% dossiers patients conformes MCDS (national)	< 10 %	≥ 60 %	≥ 70 %	**≥ 80 %**	Rapports ADD
Taux d'adoption SIH par les cliniciens (national)	Variable	≥ 55 %	≥ 65 %	**≥ 75 %**	Enquête MSPS
Volume échanges inter-GST via PNI (/ mois)	0	≥ 500	≥ 5 000	**≥ 20 000**	Logs PNI
Disponibilité PNI nationale (uptime)	N/A	≥ 99,5 %	≥ 99,7 %	**≥ 99,9 %**	DGSSI
Délai moyen d'accès au dossier patient inter-GST	Non mesuré	< 2h	< 45 min	**< 20 min**	Logs PNI
% GST certifiés ISO 27001 ou en cours	0 %	25 %	60 %	**100 %**	DGSSI

Nb d'incidents de sécurité critiques (/ an)	Non mesuré	< 10	< 5	**< 2**	Rapports DGSSI
Taux de couverture nationale programme formation	< 15 %	≥ 40 %	≥ 70 %	**≥ 90 %**	MSPS/ MESRSI
Score satisfaction utilisateurs SIH (/ 5)	Non mesuré	≥ 3,0	≥ 3,5	**≥ 4,0**	Enquête annuelle

Préparation organisationnelle transversale — Leviers activés dès Phase 1

Alignement technologie-organisation	Engagement des parties prenantes	Compétences en IA et données	Littératie numérique et formation continue
Évaluation de la cohérence outils-processus métier à chaque phase. Outil : cartographie des flux métier (BPM) produite en Phase 1 et mise à jour annuellement.	Comité des parties prenantes (direction, soignants, administratifs, représentants patients) convoqué à chaque jalon. Mécanisme de remontée des préoccupations terrain formalisé.	Module 4 déployé dès Phase 1. Création d'un Comité d'éthique de l'IA en santé (MSPS + CNDP) opérationnel à M12. Charte éthique publiée.	Module 6 obligatoire pour tout le personnel dès Phase 1. GST pilotes certifiés centres de formation régionaux à M36. Plateforme e-learning nationale accessible 24/7.

Synthèse exécutive

La présente feuille de route opérationnelle constitue le cadre de mise en œuvre de la transformation numérique hospitalière au Maroc pour la période 2025–2030. Elle repose sur une logique de progression maîtrisée en quatre phases interdépendantes, assorties d'indicateurs de performance mesurables, d'une gouvernance institutionnelle clairement répartie et d'un registre des risques opérationnel.

Les facteurs critiques de succès identifiés sont au nombre de cinq :

- La coordination sans défaillance entre MSPS, ADD, CNDP, DGSSI et ANRT, pilotée par un Comité de pilotage national réuni mensuellement.
- La qualité et la rigueur de la Phase 1 : un pilote insuffisamment documenté compromet la reproductibilité à grande échelle.
- L'investissement continu dans le capital humain : aucune infrastructure technique ne peut compenser un déficit de compétences.

- La prise en compte des inégalités territoriales dès la conception, et non comme correctif tardif.
- La transparence et la redevabilité publique, via la publication annuelle des KPIs et les rapports d'évaluation indépendants.

Le succès de cette feuille de route positionnera le Maroc comme référence régionale en matière de gouvernance numérique hospitalière, en cohérence avec les engagements de la Stratégie Digital Morocco 2030 et les standards internationaux promus par l'OMS, l'OCDE et la Banque mondiale.

CONCLUSION:

Pour le succès de la création d'un référentiel stratégique pour les GST pour un cadre national de gouvernance des données de santé, une mise en œuvre d'un cadre robuste de qualité de gouvernance des données cliniques constitue un point fondamental, répondant simultanément aux impératifs de sécurité, de fiabilité et d'interopérabilité des données de santé, ce chapitre répond à des questions cruciales et propose des recommandations pour assurer et définir un modèle organisationnel clair de gestion des données.

La gouvernance des données de santé repose sur la sécurité de ces données. C'est un élément intégral de l'architecture, en plus d'autres mesures comme le chiffrement de bout en bout (AES-256, TLS 1.3) et l'utilisation des modèles d'accès stricts (RBAC/ABAC, *Proxy Query Agent*). Cette sécurité rigoureuse est un aspect crucial pour gagner et maintenir la confiance des citoyens et des professionnels. Notre approche va au-delà d'une simple protection technique, Elle repose sur la confiance publique, et prend fortement en compte la sensibilité des données médicales. Le cadre de gouvernance inclut la sécurité par conception, le chiffrement et une traçabilité impeccable pour respecter les exigences de la CNDP . Cette sécurité solide et indispensable pour la transformation institutionnelle et la légitimité de l'intelligence artificielle en santé. Elle ne protège pas seulement le patient mais aussi l'institution, tout en favorisant la coopération transfrontalière dans un cadre de confiance mutuelle et selon des standards partagés.

La qualité et la fiabilité dépendent d'une gouvernance opérationnelle. La définition d'un MCDS et l'établissement de processus standardisés garantit que les données alimentent les EDS. Enfin, l'interopérabilité et l'accès sont essentiels pour créer de la valeur. La convergence n'entrave pas, mais organise les échanges. Un ensemble de standards clairs et des processus d'échange définis éliminent les silos et assurent une circulation sécurisée et éthique des données. L'intégration opérationnelle du cadre dans les workflows des GST et des hôpitaux, soutenue par des outils de diffusion et de sensibilisation, fait de l'interopérabilité une réalité pratique. L'EDS au niveau du GST en est un exemple : un point d'accès unifié, gouverné et sécurisé, qui sert la recherche et la prise de décision publique, tout en restant sous le contrôle des instituts sanitaires marocains.

La gouvernance des données cliniques garantit que les données, bien protégées et de haute qualité, deviennent un bien commun interopérable. Cela peut soutenir une politique nationale de santé ambitieuse, novatrice et méritant la confiance des citoyens. Mettre en œuvre ce cadre clair et opérationnel est la dernière étape pour passer des principes à l'action, transformant les données en un levier stratégique pour la santé au Maroc.

Méthodologie d'élaboration des recommandations

Les recommandations formulées dans ce référentiel reposent sur une combinaison de revue de littérature et de consultation d'experts. La revue documentaire a couvert des publications scientifiques et institutionnelles récentes, issues de bases de données académiques et de rapports d'organisations de référence sur le sujet. Elle a été complétée par des échanges avec des experts issus des domaines de la santé publique, du droit numérique et de la gouvernance hospitalière. La sélection des sources a été guidée par leur pertinence thématique et leur crédibilité institutionnelle, sans application de critères formels d'inclusion, en cohérence avec la nature stratégique du document. Le lien entre les données probantes et les orientations proposées est explicite et traçable à travers les références bibliographiques. Le projet a été soumis à une révision critique par des experts extérieurs au groupe de travail avant publication. Le groupe d'auteurs est pluridisciplinaire, avec des profils identifiés en page éditoriale. Les divergences de vues ont été résolues par discussion collégiale. Le présent référentiel n'est pas assorti d'une procédure formelle de mise à jour ; une révision est cependant recommandée dans un délai de deux à trois ans, ou en cas d'évolution substantielle du cadre réglementaire national ou international.

Conflits d'intérêt

L'équipe éditorial déclare n'avoir aucun conflit d'intérêt en lien avec le contenu de ce référentiel. Aucun financement externe n'a été mobilisé pour son élaboration.

BIBLIOGRAPHIE

[1] Da., n° 1-09-15, 22 Safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, *BO* n° 5714, 5 mars 2009, version française, art. 1.

[2] F. MEGERLIN, « NOTION DE DONNÉE DE SANTÉ. – Dynamiques conceptuelles et compétitives », *Litec Droit médical et hospitalier*, Fasc. 160-10, sept. 2023, n° 4 et 6.

[3] M. BRAKNI, J.-B. BEUSCART, H. GORGE, N. ÖZÇAĞLAR-TOULOUSE et P. QUINDROIT, « Impact de la collecte et de l'exploitation des données dans l'évolution des interactions organisationnelles dans le domaine de la santé », *21èmes Journées Normandes de Recherche sur la Consommation*, Le Havre, nov. 2022, p. 5.

[4] M. BRAKNI, J.-B. BEUSCART, H. GORGE, N. ÖZÇAĞLAR-TOULOUSE et P. QUINDROIT, op. cit., p. 5.

[5] A. TORAB-MIANDOAB, T. SAMAD-SOLTANI, A. JODATI et P. REZAEI-HACHESU, « Interoperability of heterogeneous health information systems: a systematic literature review », *BMC Medical Informatics and Decision Making*, vol. 23, n° 18, 2023, p. 2.

[6] Conseil Économique, Social et Environnemental, *La gouvernance territoriale : Levier de développement équitable et durable*, Avis n° 42, 2019, p. 6.

[7] A. TORAB-MIANDOAB, T. SAMAD-SOLTANI, A. JODATI et P. REZAEI-HACHESU, op. cit., p. 2.

[8] A. LUTUN, *Le big data en santé. Richesse et conditions d'accès*, th. Paris, dir. A. Debet, 2021, p. 53.

[9] M. CHAACHOUA, « Les enjeux des données personnelles à l'ère de l'intelligence artificielle », *REMAPP*, vol. 2, n° 28, juin 2025, p. 46.

[10] M. CHAACHOUA, op. cit., p. 46.

[11] SVENSSON-RANALLO P.A., ADAM T.J., SAINFORT F., « A framework and standardized methodology for developing minimum clinical datasets », *AMIA Joint Summits on Translational Science*, 2011, p. 54–58.

[12] KWOK C.S., MUNTEAN E.A., MALLEN C.D., BOROVAC J.A., « Data Collection Theory in Healthcare Research: The Minimum Dataset in Quantitative Studies », *Clinics and Practice*, 2022, vol. 12, n° 6, p. 832–844.

[13] HUFSTEDLER H., ROELL Y., ANDRESSA PEÑA, KRISHNAN A., GREEN I., ADRIANO BARBOSA-SILVA et al., « Navigating data standards in public health: A brief report from a data-standards meeting », *Journal of Global Health*, 2024, vol. 14.

[14] GUERIN J., YEC'HAN LAIZET, VINCENT LE TEXIER, LAETITIA CHANAS, RANCE B., KOEPPEL F. et al., « OSIRIS: A Minimum Data Set for Data Sharing and Interoperability in Oncology », *JCO Clinical Cancer Informatics*, 2021, n° 5, p. 256–265.

[15] Health Data Hub, *Une plateforme pour faire avancer la science*, MSD Connect, 2025.

[16] CUGGIA M., COMBES S., « The French Health Data Hub and the German Medical Informatics Initiatives: Two National Projects to Promote Data Sharing in Healthcare », *Yearbook of Medical Informatics*, 2019, vol. 28, n° 1, p. 195–202.

[17] Ministère des Solidarités et de la Santé (FR), *Programme de médicalisation des systèmes d'information (PMSI)*, sante.gouv.fr, 28 nov. 2017.

[18] Health Data Hub, *Standardisation du socle : note de synthèse*.

[19] *Doctrine technique du numérique en santé*, Ministère des Solidarités et de la Santé, Délégation ministérielle du numérique en santé, Paris, janv. 2021.

[20] Health Data Hub, *Rapport annuel 2022*, Paris, mars 2023.

[21] Da., n° 1-09-15, 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, *Bulletin officiel du Royaume du Maroc*, n° 5714, 5 mars 2009, version française.

[22] Dahir n° 1-20-69 du 4 hija 1441 (25 juillet 2020) portant promulgation de la loi n° 05-20 relative à la cybersécurité, *Bulletin officiel du Royaume du Maroc*, version française.

[23] Health Data Hub, *Note à l'attention du Comité Stratégique du Système National des Données de Santé : définition d'un socle de données commun aux entrepôts de données de santé hospitaliers*, Paris, 25 sept. 2023.

[24] Health Data Hub, *Formation Nomenclatures SNDS : CIM-10*, 2025.

[25] PARK H.A., « Why Terminology Standards Matter for Data-driven Artificial Intelligence in Healthcare », *Annals of Laboratory Medicine*, 3 juill. 2024.

[26] BODENREIDER O., CORNET R., VREEMAN D., « Recent Developments in Clinical Terminologies — SNOMED CT, LOINC, and RxNorm », *Yearbook of Medical Informatics*, 2018, vol. 27, n° 1, p. 129–139.

[27] HOLLIS K., « To Share or Not to Share: Ethical Acquisition and Use of Medical Data », *AMIA Summits on Translational Science Proceedings*, 2016. Disponible sur : https://www.semanticscholar.org/paper/4487c890a15889b2107131b87a6a2f9184375c4f

[28] CHEN H., HAILEY D., WANG N., YU R., « A Review of Data Quality Assessment Methods for Public Health Information Systems », *International Journal of Environmental Research and Public Health*, 2014, vol. 11, n° 5, p. 5170–5207. Disponible sur : https://www.mdpi.com/1660-4601/11/5/5170

[29] HAEGEMANS T., SNOECK M., LEMAHIEU W., « Towards a Precise Definition of Data Accuracy and a Justification for its Measure », 2016. Disponible sur : https://www.semanticscholar.org/paper/0cae60d5683fc3b4ba63b82a5847e6f047511156

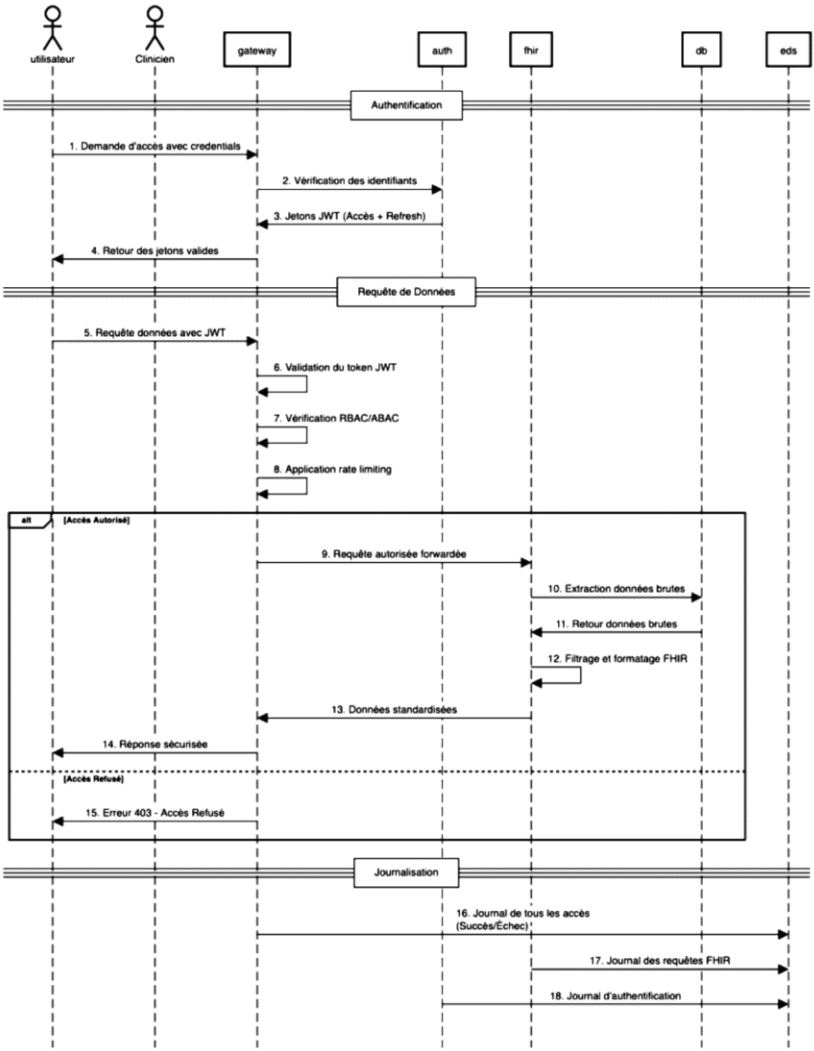
[30] Royaume du Maroc, *Loi-cadre n° 06-22 relative au système national de santé*, 2024. Disponible sur : https://amdie.gov.ma/wp-content/uploads/2024/02/Loi-cadre-n%C2%B0-06-22-relative-au-systeme-national-de-sante.pdf
[31] ISSAOUI A., ÖRTENSJÖ J., ISLAM M.S., « Exploring the General Data Protection Regulation (GDPR) compliance in cloud services: insights from Swedish public organizations on privacy compliance », *Future Business Journal*, 2023, vol. 9, n° 107. Disponible sur : https://doi.org/10.1186/s43093-023-00285-2
[32] CNDP, *IA et protection des données à caractère personnel*, Communiqué de presse, 18 mars 2025. Disponible sur : https://www.cndp.ma/ia-et-protection-des-donnees-a-caractere-personnel/
[33] CESE, *Quels usages et quelles perspectives de développement de l'intelligence artificielle au Maroc ?*, Avis n° 78/2024.
[34] E. ADNANI, A. HAOUNANI, « L'intelligence Artificielle au Maroc : Entre éthique et réglementation », *Revue-IRS*, vol. 2, n° 3, juin 2024, p. 1238.
[35] Loi française n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024.
[36] Projet de Loi canadienne sur l'intelligence artificielle et les données (LIAD).
[37] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (AI Act).
[38] É. DEBAETS, « Big data en sciences sociales et protection des données personnelles », in V. GINOUVÈS et I. GRAS (dir.), *La diffusion numérique des données en SHS. Guide des bonnes pratiques éthiques et juridiques*, Presses universitaires de Provence, 2018, p. 61.
[39] Conseil d'État, *Le numérique et les droits fondamentaux*, Étude annuelle 2014, La documentation française, 2014, p. 48.
[40] M. BOUHRIZ, H. CHAOUI, « Big Data Privacy in Healthcare Moroccan context », *Procedia Computer Science*, vol. 63, Elsevier, 2015, p. 576.
[41] M. BOUHRIZ, H. CHAOUI, op. cit., p. 576.
[42] D. WIEPERT, B.A. MALIN, J.R. DUFFY, R.L. UTIANSKI, J.L. STRICKER, D.T. JONES et H. BOTHA, « Reidentification of Participants in Shared Clinical Data Sets: Experimental Study », *JMIR AI*, vol. 3, 2024. Disponible sur : https://doi.org/10.2196/52054
[43] S. VULLIET-TAVERNIER, « BigData et protection des données personnelles : quels enjeux ? Éléments de réflexion », *Statistique et société*, n° 2, déc. 2014, p. 27–31.
[44] M. CHAACHOUA et N. ABA, « Les enjeux des données personnelles à l'ère de l'intelligence artificielle », *REMAPP*, vol. 2, n° 28, juin 2025, p. 44.
[45] L. n° 09-08, art. 27 – art. 31.
[46] M. CHAACHOUA et N. ABA, op. cit., p. 45.
[47] Avis du Conseil Économique, Social et Environnemental, « Vers une transformation digitale responsable et inclusive », n° 52, 2021. Disponible sur : https://www.cese.ma/docs/vers-une-transformation-digitale-responsable-et-inclusive/#downloads
[48] Da., n° 1-10-15, 26 safar 1431 (11 février 2010) portant promulgation de la loi n° 12-06 relative à la normalisation, à la certification et à l'accréditation, *BO* n° 5822, 18 mars 2010, p. 222, version française.
[49] L. n° 12-06, art. 1er.
[50] L. n° 12-06, art. 2.
[51] CNDP, *Communiqué de presse : La normalisation au service de la protection des données à caractère personnel*. Disponible sur : https://www.cndp.ma/communique-de-presse-la-normalisation-au-service-de-la-protection-des-donnees-a-caractere-personnel/
[52] N. ROUINI et A. EL AIDOUNI, « Analyse comparative de la réglementation sur la protection des données à caractère personnel entre le Maroc et l'UE », *RDCEC*, vol. 4, n° 2, 2023, p. 34. — M. CHAACHOUA et N. ABA, op. cit., p. 45.
[53] N. ROUINI et A. EL AIDOUNI, op. cit., p. 34.
[54] CNIL, « La CNIL à Montpellier pour sensibiliser à la protection des données personnelles », 26 nov. 2024. Disponible sur : https://www.cnil.fr/fr/la-cnil-montpellier-pour-sensibiliser-la-protection-des-donnees-personnelles
[55] ISO/IEC 27701:2025, *Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la protection de la vie privée — Exigences et recommandations*. Disponible sur : https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27701:ed-2:v1:fr
[56] CNIL, *Le règlement général sur la protection des données — RGPD. Chapitre IV — Responsable du traitement et sous-traitant*. Disponible sur : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4
[57] ALM, « Protection des données à caractère personnel : La CNDP et l'Imanor s'allient pour la "marocanisation" des normes internationales », juill. 2021. Disponible sur : https://aujourdhui.ma/high-tech/protection-des-donnees-a-caractere-personnel-la-cndp-et-limanor-sallient-pour-la-marocanisation-des-normes-internationales
[58] L. n° 09-08, art. 51.
[59] N. ROUINI et A. EL AIDOUNI, op. cit., p. 28.
[60] O. SEGHROUCHNI, « CNDP : perspectives stratégiques pour renforcer la protection et la conformité des données personnelles au Maroc », *La lettre d'Artémis*, n° 34, 1er trimestre 2025, p. 11–12.
[61] Site officiel du ministère de la Santé et de la Protection Sociale, rubrique DIM [consulté le 25/12/2025].
[62] Site officiel du Groupement Sanitaire Territorial de Tanger-Tétouan-Al Hoceima [consulté le 08/01/2026].
[63] The World Bank, *Implementation Completion and Results Report IBRD-85070 and IBRD-91470 on a Loan in the Amount of US$135 Million to the Kingdom of Morocco for the Improving Primary Health in Rural Areas and Responding to COVID-19 Pandemic Emergency Program-for-Results*, Report n° ICR00005682, 29 juin 2022.

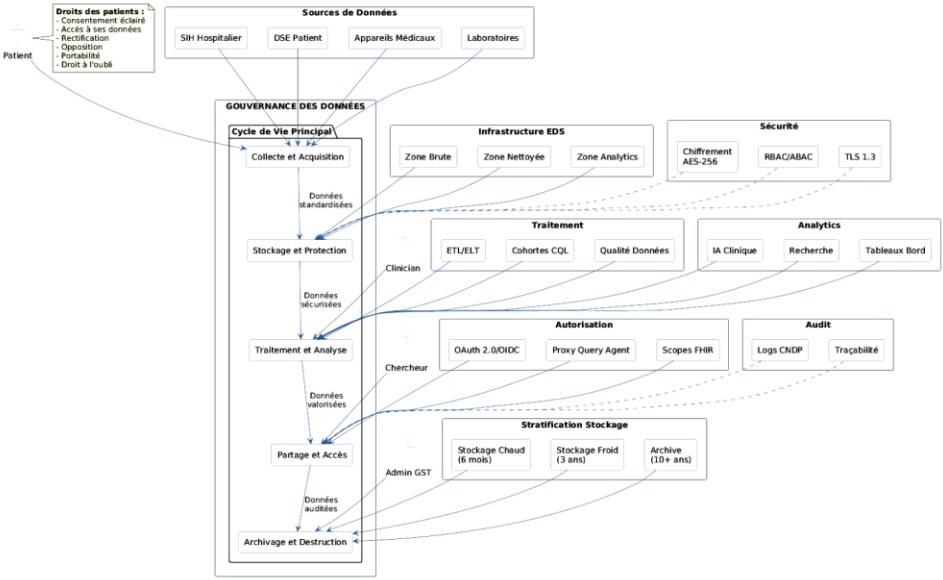
[64] The World Bank, op. cit.
[65] OECD, *Health Data Governance for the Digital Age: Implementing the OECD Recommendation on Health Data Governance*, OECD Publishing, Paris, 2022. Disponible sur : https://doi.org/10.1787/68b60796-en
[66] Organisation internationale de normalisation (ISO), *Famille ISO/IEC 27000 — Management de la sécurité de l'information*, Genève, 2025. Disponible sur : https://www.iso.org/fr/standard/iso-iec-27000-family
[67] World Bank, *Implementation Status & Results Report: Morocco Health Reform Program (P179014)*, ISR03974, Washington DC, 2025.
[68] Direction générale de la sécurité des systèmes d'information, *Référentiel de gestion des incidents de cybersécurité*, éd. 2022.
[69] World Bank, *Digital-in-Health: Unlocking the Value for Everyone*, Washington DC, 2023. Licence : CC BY 4.0.
[70] World Bank, *Document d'évaluation du programme relatif à un prêt proposé pour un montant de 450 millions de dollars américains au Royaume du Maroc pour le Programme pour les résultats pour l'appui à la refonte du système de santé au Maroc*, Report n° PAD5318, 24 mai 2023.
[71] World Health Organization, *Global strategy on digital health 2020–2025*, Geneva, 2021. Licence : CC BY-NC-SA 3.0 IGO.
[72] National Health Service (NHS) England, *Standard Operating Procedures for Risk Management and Incident Reporting*, 2021. — OMS et OCDE, *Ethical Governance of Artificial Intelligence for Health*, 2021.
[73] Health and Safety Executive (HSE), *Risk Assessment Template and Examples*, 2022.
[74] Ministère de la Transition Numérique et de la Réforme de l'Administration, *Stratégie Digital Morocco 2030*, 2023.
[75] Ministère de la Transition Numérique et de la Réforme de l'Administration, op. cit.
[76] International Organization for Standardization (ISO), *ISO/IEC 27001: Information Security Management Systems — Requirements*, 2013.
[77] International Organization for Standardization (ISO), op. cit.
[78] International Organization for Standardization (ISO), op. cit.
[79] International Organization for Standardization (ISO), op. cit. — OMS et OCDE, *Ethical Governance of Artificial Intelligence for Health*, 2021.
[80] International Organization for Standardization (ISO), *ISO/IEC 27001: Information Security Management Systems — Requirements*, 2013.
[81] World Health Organization, *Guidance on Ethics and Governance of Artificial Intelligence for Health*, Geneva, WHO, 2021.
[82] World Health Organization, *Ethics and governance of artificial intelligence for health*, Geneva, WHO, 2021.
[83] World Health Organization, *Health data governance in the age of artificial intelligence: policy imperatives*, Geneva, WHO.
[84] OCDE, *Gouvernance des données de santé à l'ère du numérique*, OCDE Publishing, Paris.
[85] World Health Organization, *Health data governance in the age of artificial intelligence: policy imperatives*, Geneva, WHO.
[86] World Health Organization, *Ethics and governance of artificial intelligence for health*, Geneva, WHO, 2021.
[87] ISO/IEC 27701:2019, *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*.
[88] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD), art. 38 et 39.
[89] European Data Protection Board (EDPB), *Guidelines on Data Protection Officers*, 2022.
[90] World Health Organization, *Ethics and governance of artificial intelligence for health*, Geneva, WHO, 2021.
[91] OCDE, *Gouvernance des données de santé à l'ère du numérique*, OCDE Publishing, Paris.
[92] World Health Organization, *Ethics and governance of artificial intelligence for health*, Geneva, WHO, 2021.
[93] OCDE, *Gouvernance des données de santé à l'ère du numérique*, OCDE Publishing, Paris.
[94] World Health Organization, *Health data governance in the age of artificial intelligence: policy imperatives*, Geneva, WHO.
[95] World Health Organization, op. cit.
[96] OCDE, *Gouvernance des données de santé à l'ère du numérique*, OCDE Publishing, Paris.
[97] World Health Organization, *Ethics and governance of artificial intelligence for health*, Geneva, WHO, 2021.
[98] OCDE, *Gouvernance des données de santé à l'ère du numérique*, OCDE Publishing, Paris.
[99] World Health Organization, *Health data governance in the age of artificial intelligence: policy imperatives*, Geneva, WHO.
[100] World Health Organization, op. cit.
[101] CNDP, *Rapport sur la protection des données personnelles et l'éthique de l'IA*, 2023.
[102] World Health Organization, *Ethics and governance of artificial intelligence for health*, Geneva, WHO, 2021.
[103] OECD, *Digital Government Index: Health Sector Insights*, 2022.
[104] Ministère de la Transition Numérique et de la Réforme de l'Administration, *Stratégie nationale de digitalisation du système de santé*, Rabat, 2023.
[105] Loi-cadre n° 06-22 relative au système de santé, Maroc, 2022.
[106] Ministère de la Santé, Maroc, *Dossier Médical Partagé et interopérabilité des systèmes de santé*, Rabat, 2023.
[107] World Bank, *Morocco Health System Reform Program (P179014)*, Washington DC, 2023.
[108] Loi-cadre n° 06-22 relative au système de santé, Maroc, 2022.
[109] Ministère de la Transition Numérique et de la Réforme de l'Administration, *Stratégie nationale de digitalisation du système de santé*, Rabat, 2023.
[110] CNIL, *Cartographie des EDS en France* [consulté le 23 décembre 2025]. Disponible sur : https://carto-eds.beta.cnil.fr/
[111] Portail data.gov.ma, *Open Data Maroc — Groupe Santé* [consulté le 23 décembre 2025]. Disponible sur : https://www.data.gov.ma

[112] France. Arrêté du 29 juin 2021 portant création du Comité stratégique des données de santé. *Légifrance*, 2021. Disponible sur : https://www.legifrance.gouv.fr

TABLE DES ANNEXES

Annexe	Intitulé	Page
Annexe I-1	Architecture de circulation des données fondée sur le modèle Zero Trust	**25**
Annexe I-2	Modèle recommandé de cycle de vie des données hospitalières	**29**





ABRÉVIATIONS ET ACRONYMES

Sigle	Signification
ADD	Agence de Développement Digital
AMO	Assurance Maladie Obligatoire
ANRT	Agence Nationale de Réglementation des Télécommunications
APD	Autorité de Protection des Données
CHU	Centre Hospitalier Universitaire
CIM-10	Classification Internationale des Maladies, 10e révision
CNDP	Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel
CNIL	Commission Nationale de l'Informatique et des Libertés (France)
CNDS	Comité National des Données de Santé
CSNCA	Conseil Supérieur de Certification et d'Accréditation
DGSSI	Direction Générale de la Sécurité des Systèmes d'Information
DIM	Division de l'Informatique et des Méthodes
DMP	Dossier Médical Partagé
DPO / DPD	Data Protection Officer / Délégué à la Protection des Données

DSI	Direction des Systèmes d'Information
EDS / EDSH	Entrepôt de Données de Santé (Hospitalier)
GST	Groupement Sanitaire Territorial
HDH	Health Data Hub (France)
HL7 FHIR	Health Level 7 – Fast Healthcare Interoperability Resources
IMANOR	Institut Marocain de Normalisation
ISO	Organisation Internationale de Normalisation
LOINC	Logical Observation Identifiers Names and Codes
MCDS	Minimum Clinical Data Set / Socle Minimal des Données Cliniques
MESRSI	Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et de l'Innovation
MPI	Master Patient Index / Identifiant Patient Unique
MSPS	Ministère de la Santé et de la Protection Sociale
OCDE	Organisation de Coopération et de Développement Économiques
OMS	Organisation Mondiale de la Santé
RGPD	Règlement Général sur la Protection des Données (UE)
SIH	Système d'Information Hospitalier
SNOMED CT	Systematized Nomenclature of Medicine – Clinical Terms